#3

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of	: **Ikuya MORIKAWA**
Filed:	: **Concurrently herewith**
For:	: **DISTRIBUTED ENVIRONMENT TYPE.....**
Serial No.	: **Concurrently herewith**

Assistant Commissioner for Patents
Washington, D.C. 20231

February 5, 2002

PRIORITY CLAIM AND SUBMISSION

OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from **JAPANESE** patent application no. **2001-165452** filed **May 31, 2001,** a certified copy of which is enclosed.

Any fee, due as a result of this paper, not covered by an enclosed check, may be charged to Deposit Acct. No. 50-1290.

Respectfully submitted,

Thomas J. Bean
Reg. No. 44,528

ROSENMAN & COLIN, LLP
575 MADISON AVENUE
IP Department
NEW YORK, NEW YORK 10022-2584
DOCKET NO.: FUJA 19.410
TELEPHONE: (212) 940-8800

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　５月３１日

出願番号
Application Number: 特願２００１－１６５４５２

出願人
Applicant(s): 富士通株式会社

２００１年１０月１９日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０９２８５７

【書類名】　特許願

【整理番号】　0150931

【提出日】　平成13年 5月31日

【あて先】　特許庁長官　及川　耕造　殿

【国際特許分類】　G06F 13/00

【発明の名称】　コンピュータシステム、サービス層、ポリシーキャッシュ機能部およびポリシー管理装置

【請求項の数】　10

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　森川　郁也

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100077517

【弁理士】

【氏名又は名称】　石田　敬

【電話番号】　03-5470-1900

【選任した代理人】

【識別番号】　100092624

【弁理士】

【氏名又は名称】　鶴田　準一

【選任した代理人】

【識別番号】　100100871

【弁理士】

【氏名又は名称】　土屋　繁

【選任した代理人】

【識別番号】　100082898

【弁理士】

【氏名又は名称】　西山　雅也

【選任した代理人】

【識別番号】　100081330

【弁理士】

【氏名又は名称】　樋口　外治

【手数料の表示】

【予納台帳番号】　036135

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9905449

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　コンピュータシステム、サービス層、ポリシーキャッシュ機能部およびポリシー管理装置

【特許請求の範囲】

【請求項１】　アプリケーションに基づいて一連のメッセージを送受信するメッセージ送受信手段と、

各前記メッセージに対して特定の制御または指示を与えるためのポリシーに従って、前記アプリケーションに対し特定の付加的サービスを提供するサービス層と、

種々の前記ポリシーを保持して一括管理し、前記サービス層からの取得の要求に応じて、前記メッセージに対応する前記ポリシーを供給するポリシー管理装置と、

前記サービス層により、前記ポリシーに従って前記サービスが付加された前記メッセージを、相手方アプリケーションとの間でやりとりする通信層と、を備えるコンピュータシステムにおいて、

前記サービス層内に、

各前記メッセージを特定するために各該メッセージに記述されるパラメータを、比較的長時間にわたって変化しない静的パラメータと比較的短時間で変化する動的パラメータとに区分して、各該メッセージより抽出する解析手段と、

抽出された前記静的パラメータを用いて、前記ポリシー管理装置に対し、該静的パラメータに割り当てられたポリシー群の取得を要求する要求手段と、を形成することを特徴とするコンピュータシステム。

【請求項２】　前記ポリシー管理装置は、前記要求手段から前記静的パラメータを用いて前記の取得の要求を受けたとき、ポリシークラスタを生成して該要求手段に返送する応答機能部を有し、ここに、該ポリシークラスタは、該静的パラメータと種々変化する各動的パラメータとを合成してなる全体パラメータの各々に対応するポリシー群と、該全体パラメータの各々に対する該ポリシー群の各々の割り当てを示すポリシー割り当て規則と、を少なくとも含んで構成されることを特徴とする請求項１に記載のコンピュータシステム。

【請求項３】　前記要求手段はポリシーキャッシュ機能部を有し該ポリシーキャッシュ機能部は、前記ポリシー管理装置から返送された前記ポリシークラスタを、読み出し自在に、一時的に保存し、前記メッセージの送受信開始後は、送信した前記全体パラメータに割り当てられた前記ポリシークラスタが該ポリシーキャッシュ機能部に保存されているときはここから当該ポリシーを取得することを特徴とする請求項２に記載のコンピュータシステム。

【請求項４】　前記要求手段は、前記ポリシー管理装置から前記ポリシークラスタを取得した際に、該ポリシークラスタ内に表示された前記署名が正当であることを検証するための署名検証機能部を有することを特徴とする請求項２に記載のコンピュータシステム。

【請求項５】　アプリケーションに基づいて送受信される一連のメッセージに対し、外部のポリシー管理装置と連係しながら、ポリシーに従って特定の付加的サービスを提供するサービス層であって、

該サービス層は、

各前記メッセージを特定するために各該メッセージに記述されるパラメータを、比較的長時間にわたって変化しない静的パラメータと比較的短時間で変化する動的パラメータとに区分して、各該メッセージより抽出する解析手段と、

抽出された前記静的パラメータを用いて、前記ポリシー管理装置に対し、該静的パラメータに割り当てられたポリシー群の取得を要求する要求手段と、

を有することを特徴とするサービス層。

【請求項６】　前記解析手段は、前記静的パラメータを抽出する静的パラメータ解析機能部と前記動的パラメータを抽出する動的パラメータ解析機能部と、からなることを特徴とする請求項５に記載のサービス層。

【請求項７】　アプリケーションに基づいて送受信される一連のメッセージに対し、外部のポリシー管理装置と連係しながら、ポリシーに従って特定の付加的サービスを提供するサービス層内に設けられるポリシーキャッシュ機能部であって、

該ポリシーキャッシュ機能部は、

各前記メッセージに対して特定の制御または指示を与えるための１または複数

のポリシーを、前記ポリシー管理装置から取得して一時的に格納するキャッシュメモリと、

前記ポリシーを格納した前記キャッシュメモリ内の格納位置を各ポリシー対応に記録するポリシーキャッシュテーブルと、

各前記メッセージを特定するために各該メッセージに記述されるパラメータの各々に対する前記ポリシーの割り当て規則を定める割り当て規則キャッシュテーブルと、

を有することを特徴とするポリシーキャッシュ機能部。

【請求項８】　前記割り当て規則キャッシュテーブルは、前記メッセージを送受信する相手方アプリケーションをサポートするサービス層との間で事前に交渉して、両者間で適用すべきポリシーについて合意したとき、前記割り当て規則キャッシュテーブル内に記録された各前記ポリシーについて合意があったことを表示するための交渉済みフラグ領域を含むことを特徴とする請求項７に記載のポリシーキャッシュ機能部。

【請求項９】　アプリケーションに基づいて送受信される一連のメッセージに対し特定の付加的サービスを提供するサービス層と連係し、各前記メッセージに対して特定の制御または指示を与えるための１または複数のポリシーを該サービス層に供給するためのポリシー管理装置であって、

該ポリシー管理装置は、

前記サービス層にて、各前記メッセージを特定するために各該メッセージに記述されるパラメータを、比較的長時間にわたって変化しない静的パラメータと比較的短時間で変化する動的パラメータとに区分して得たパラメータのうち該静的パラメータをもって、該サービス層より、前記ポリシーの取得が要求されたとき、ポリシークラスタを生成して該サービス層に返送する応答機能部を有し、

ここに、該ポリシークラスタは、該静的パラメータと種々変化する各動的パラメータとを合成してなる全体パラメータの各々に対応するポリシー群と、該全体パラメータの各々に対する該ポリシー群の各々の割り当てを示すポリシー割り当て規則と、を少なくとも含んで構成されることを特徴とするポリシー管理装置。

【請求項１０】　前記メッセージの送受信を行う相手方アプリケーションを

サポートする相手方ポリシー管理装置との間で事前に交渉して、両者間で適用すべきポリシーについて合意したとき、合意があったことを、前記ポリシークラスタ内において記録するための交渉済みタグを生成する事前交渉機能部を有することを特徴とする請求項９に記載のポリシー管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、分散環境のもとでアプリケーションソフトウェアに従ってメッセージのやりとりを行う複数のコンピュータシステムに関し、さらに、各コンピュータシステムに組み込まれて、ポリシーに従い、付加的サービスを提供するサービス層およびこのサービス層に連係して上記のポリシーを集中管理するポリシー管理装置に関する。

【０００２】

近年のコンピュータネットワークの発展により、分散して存在する複数のコンピュータシステムの間で、アプリケーションソフトウェアに従って互いに情報をやりとりすることが広く行われるようになってきた。このような環境を一般に分散環境と呼ぶ。

このような分散環境では、応用的な機能を提供するアプリケーションソフトウェアと、通信に関する機能を汎用的に提供する通信層とを分離して実現するということが広く行われるようになった。ここに通信層は、物理的な通信機能すなわち通信回線や通信ネットワークと、そのような物理的な通信機能を通信手順として規則化した通信プロトコルと、この通信プロトコルをアプリケーションソフトウェアに提供するためのオペレーティングシステム（ＯＳ）やアプリケーションプログラミングインタフェース（ＡＰＩ）と、さらに高度な通信機能や通信補助機能を内包した分散プラットフォーム層（ＤＰＬ：Distributed Platform Layer）等を含む。このＤＰＬの代表的な例としては、ＯＳよりもさらに豊富な通信機能を提供するいわゆる共通オブジェクト要求ブローカーアーキテクチャ(Common Object Request Broker Architecture；ＣＯＲＢＡ）を挙げることができる。

【０００３】

【従来の技術】

図１２は既に提案されている、分散環境型のコンピュータシステムを示す図（その１）、

図１３は同図（その２）である。

まず始めに、これら図１２および図１３に示す分散環境型のコンピュータシステムの概要について説明する。

【０００４】

前述したような分散環境において、図１２および図１３のシステム構成は、ある通信層（５，６）とアプリケーションソフトウェア（１，２）との間に存在し、その通信層では実現できない付加的サービスを提供するサービス層（３，４）を導入することを１つの特徴としている。

このサービス層は、通信層とアプリケーションソフトウェアの両者から独立して、付加的サービスを提供する。これにより、通信層およびアプリケーションソフトウェア双方の汎用性を保ちつつ、アプリケーションソフトウェアの開発の手間を省くことができる。この点でサービス層は有益である。なおこのようなサービス層自体の公知例としては、下記参考文献１で開示されているＣＯＲＢＡセキュリティサービスがある。

【０００５】

参考文献１：Object Management Group(ＯＭＧ)，ＣＯＲＢＡservices：Security Service Specification, Version 1.7, December 1999.
(http://www.omg.org/technology/documents/formal/security#service.htm より入手可能)

さらに図１２および図１３に示すセキュリティサービス層は、下記参考文献２、参考文献２’、参考文献２”および参考文献３で開示されている。

【０００６】

参考文献２：電子情報通信学会　第９回テレコミュニケーションマネージメント（ＴＭ）研究会（２０００年５月１８日予稿集配布）
(http://www.ieice.or.jp/cs/tm/jpn/tmken/tm-9.htmlより関連資料を入手可能)

参考文献２’：国際会議　ＡＰＮＯＭＳ２０００（２０００年５月２６日査読原稿提出、８月２５日カメラレディ原稿提出、１０月１１日予稿集配布）（http://www.ieice.or.jp/cs/tm/apnoms/2000/ より関連資料を入手可能）

参考文献２”：独国特許出願Ｎｏ．１００２４３４７．９（出願日２０００年５月１７日）

〔注：参考文献２，２’および２”は実質的に類似の内容である〕

参考文献３：特願２００１－５５３２３号「通信セキュリティ管理システム及びそのプログラム」（出願日２００１年２月２８日）

一般に分散環境においては、サービス層（３，４）を構成するサービス機能部分は、分散したアプリケーションソフトウェアに付随して分散して存在する。したがって、上記のサービス機能部分に、動作の仕方を外部から指示し、その指示の内容を管理領域（管理すべき一単位のコンピュータシステム群）毎に一ヶ所にまとめて管理することによって、あちこちで動作の仕方を管理するという手間を省くことができ、システムの効率化を図ることができる。このような動作の仕方の指示内容は、ポリシーと呼ばれる。上記参考文献には、ポリシーによりサービス層を管理することが開示されている。

【０００７】

より具体的には、上記参考文献２，２’および２”には、サービス層（３，４）において適用するポリシーを、通信相手と交渉し決定する仕組みが述べられている。また上記参考文献３には、ポリシー管理装置（７，８）において、通信相手と相違を生じないよう事前にポリシーを交渉する仕組みが述べられている。

ここで図１２および図１３を参照する。

【０００８】

これらの図に示すように、分散環境型のコンピュータシステムは大別して、アプリケーション（アプリケーションソフトウェア）１，２、サービス層３，４、通信層５，６、およびポリシー管理装置７，８から構成される。

アプリケーション１，２は、通信層５，６を利用して、メッセージの通信を行うアプリケーションソフトウェアであり、その通信のためにメッセージ送受手段１０，２０を用いる。

【０００９】

サービス層３，４は、アプリケーション１，２と通信層５，６との間に存在し、そのアプリケーションに代わって、通信層５，６が提供することのできない付加的サービスを提供する層である。このサービス層３，４は、解析手段３０，４０と、要求手段３１，４１と、制御手段３２，４２とからなる。要求手段３１，４１は、ポリシー取得機能部３４，４４と、交渉機能部３６，４６とを具備する。

【００１０】

一方、ポリシー管理装置７，８は、ポリシー記憶領域７０，８０と、応答機能部７１，８１と、事前交渉機能部７２，８２とを具備する。

上述した図１２および図１３に示すコンピュータシステムは、上記の参考文献２，２’，２”および３に基づいて構築されたものである。このコンピュータシステムは実用に供し得るものであるが、サービス層３，４がポリシーを取得する際の処理時間ならびに通信時間が長くなってしまうという不利がある。そこで本出願人は図１４および図１５に示すコンピュータシステムを独自に考案した。

【００１１】

図１４は本発明の前提をなす分散環境型のコンピュータシステムを示す図（その１）、

図１５は同図（その２）である。

これらの図に示すとおり、本発明の前提をなす分散環境型のコンピュータシステムは、図１２および図１３に示すシステム構成に対し、さらにポリシーキャッシュ機能部３５，４５を追加したものである。

【００１２】

このように、コンピュータシステムや通信システムにおいて広く用いられている一時的な記憶領域、すなわちキャッシュの仕組みを利用すると、ポリシーを取得する際の処理時間や通信時間等を短縮でき、サービス層３，４の動作を一層高速化することができる。

ところが実際に図１４および図１５に示すコンピュータシステムを運用してみると、新たな不利が生じてしまうことが判明し（後述）、まだ十分実用的なコン

ピュータシステムまでには至っていない。すなわちさらなる改良が必要となる。この改良を加えることが本発明の主題である（後述）。

【００１３】

ここで図１４および図１５に示すシステムの動作について簡単に説明しておく。

図１６は図１４および図１５に示す本発明の前提をなすコンピュータシステムにおける処理の流れを示すフローチャート（その１）、

図１７は同フローチャート（その２）である。

【００１４】

なお本発明で扱う分散環境型のコンピュータシステムは複数のコンピュータシステムを対象とするものであるが簡素化のために２つのコンピュータシステムのみを例示することとする。またその２つのコンピュータシステムはほぼ同様の処理を行うので、アプリケーション１を扱うコンピュータシステム（図１４、図１）を代表として説明し、アプリケーション２を扱うコンピュータシステム（図１５、図２）は、単に“相手方”コンピュータシステムあるいは“相手方”アプリケーションと称することにする。

【００１５】

図１６および図１７を参照すると、アプリケーション１が、メッセージ送受手段１０を用いてアプリケーション２へメッセージを送信すると（Ｓ０１）、サービス層３の解析手段３０は、パラメータ取得機能部３３を用いてそのメッセージを解析し、サービスを制御するのに必要なパラメータをその中から抽出する（Ｓ０２）。

【００１６】

抽出したパラメータは要求手段３１へ渡され、要求手段３１はそのパラメータに対応するポリシーを取得するため、まずポリシーキャッシュ機能部３５にキャッシュされているポリシー群の中から当該ポリシーを探し（Ｓ０３）、これがなければポリシー管理装置７へ問い合わせる（Ｓ０４のＮｏ，Ｓ０５）。

ポリシー管理装置７からポリシーが得られた場合は（Ｓ０６のＹｅｓ）、それをポリシーキャッシュ機能部３５に保存する（Ｓ０７）。ポリシーが得られなけ

れば（Ｓ０６のＮｏ）、ステップＳ１１に至る。

【００１７】

次に、得られたポリシーでサービスを制御してよいか、交渉機能部３６を使って通信相手方の要求手段４１と交渉を行う（Ｓ０８）。交渉が成立すれば（Ｓ０９のＹｅｓ）、ポリシーは制御手段３２へ渡され、制御手段はそのポリシーで指定されたようにサービスを制御する（Ｓ１２）。そしてこの制御下でメッセージは通信層５および６を介して通信され、相手方アプリケーション２のメッセージ送受手段２０がそのメッセージを受け取ることができる（Ｓ１３）。

【００１８】

この場合、交渉不成立になる機会を減らすため、ポリシー管理装置７と相手方ポリシー管理装置８は、各々の事前交渉機能部７２および８２を用いて両者間で事前に交渉を行い、それぞれの応答機能部７１および８１から応答する各ポリシーを一致させておくことができる。

【００１９】

【発明が解決しようとする課題】

分散環境のある種の利用形態においては、アプリケーションは短時間の間に異なる種類のメッセージを数多く送受信する場合がある。例えば前述したＣＯＲＢＡを用いて実現された遠隔操作アプリケーションにおいては、（ｉ）別のアプリケーションの内部の状態を問い合わせるための要求を発し、（ii）処理を依頼するための要求を発し、（iii）再び問い合わせのための要求を発し、（iv）また別の処理依頼要求を発する、といったように、異なる要求を短時間内に数多く行うことが求められる場合がある。

【００２０】

このような場合に、図３および図４のシステム構成では、新しい要求（上述の諸要求）が現れるたびに、ポリシーキャッシュ機能部３５（４５）から適切なポリシーを取得できないミスいわゆるキャッシュミスが発生し、ポリシー管理装置７（８）からポリシーを取得するために余分な時間を費やしてしまう。このように、キャッシュの仕組みを持っているにも拘わらず、そのキャッシュミスにより効率的な動作ができない、という問題がある。

【００２１】

一方、上記のようなキャッシュミスに対し、一般のコンピュータシステムにおけるキャッシュでは、例えばメモリの中のある該当領域を連続して一体に取り出してキャッシュするということが行われている。これにより連続的なメモリアクセスに対するキャッシュミスを防いでおり、このようにするのが一般的である。ところが上記のポリシーキャッシュの場合においては、必要となるポリシーの群は連続していないことが多い。このため前述の一般的なキャッシュではその本来の効果を発揮できない。言い換えると、前記の場合では、必要となるポリシーを予測する適切な戦略に基づいてポリシーを取得しなければならない、という問題がある。

【００２２】

さらに図１４および図１５のシステム構成では、たとえ適切にポリシーがキャッシュされていたとしても、サービス層３はポリシー毎に通信の相手方サービス層４との間で交渉を行わなければならない。したがってその交渉のために通信時間や処理時間が必要となり、余分な時間を費やしてしまう、という問題がある。

さらに図１４および図１５のシステム構成では、ポリシー管理装置７と８の間で事前にお互いのポリシーに関する交渉を済ませて、通信中におけるサービス層３および４の間での交渉を省略するようにしているが、その事前交渉が済んでいることの信頼性を保証するための手段が実現されていない。このため、サービス層３（４）としては、ポリシー管理装置７（８）で行われた不正あるいは人為的な設定ミス、によるポリシーの不一致や、通信エラーに起因するポリシーの伝達ミス等によるポリシーの不一致が発生することを防ぐことができない。

【００２３】

このように、図１４および図１５のシステム構成では、前述したある種の利用形態において、メッセージの通信に余分な時間がかかったり、また両サービス層の間で行われるポリシーの交渉についてその交渉の信頼性が保証されていないために、利用者に不利益を与えてしまう、という問題がある。

したがって本発明は、上記の諸問題点に鑑み、サービス層３がメッセージ通信毎に行うポリシー管理装置７へのポリシーの問い合わせのための処理を大幅に減

らし、また相手方サービス層４との間で行われるポリシーの適用に関する交渉のための処理を省略することのできる、したがってサービス層３が連続したメッセージ通信を高速に実行することのできるコンピュータシステムを提供することを目的とするものである。

【００２４】

またそのコンピュータシステムのための、サービス層とポリシーキャッシュ機能部とポリシー管理装置を提供することを目的とするものである。

【００２５】

【課題を解決するための手段】

本発明において、ポリシーをキャッシュする手法として第１に、サービス層３において扱うパラメータを、「静的パラメータ」と「動的パラメータ」に区分する。静的パラメータは比較的長時間にわたって変化しないパラメータであり、動的パラメータは比較的短時間で変化するパラメータである。

【００２６】

また第２に、ポリシーキャッシュ機能部３５にキャッシュされたポリシーが、交渉済みか否かを表示するために、該機能部３５内に「交渉済みフラグ」を持つようにする。

さらに第３として、複数のポリシーを、サービス層３がポリシー管理装置７から一括して取得するために、複数のポリシーとそれらのポリシーを該当のパラメータに割り当てるための割り当て規則とを一つにまとめた「ポリシークラスタ」を利用する。

【００２７】

また第４として、ポリシー管理装置７にて生成するポリシークラスタ全体が、相手方ポリシー管理装置８と事前に交渉済みであることを示すために、ポリシークラスタ内に「交渉済みタグ」を持つようにする。この交渉済みタグは、複数のポリシー管理装置（７，８）の間で合意された値を持つ。

さらに第５として、ポリシークラスタ全体が交渉済みであることを保証するために、ポリシークラスタに「署名情報」を付与するようにする。

【００２８】

上述した第１～第５の手法を採用する本発明のコンピュータシステムによれば、以下の効果を得ることができる。

ａ）長時間にわたって変化しない静的パラメータによって、ある期間内に必要となるポリシー群を、戦略的にキャッシュすることができる。このため、キャッシュミスの頻度が下がり、メッセージを通信するのに要する時間を短縮することが可能となる。

【００２９】

ｂ）また、すでに交渉済みであるポリシーを、ポリシーキャッシュ機能部３５内の前記交渉済みフラグによって印づけることによって、２度目以降に行うべき交渉を省略することができ、このためメッセージ通信するのに必要とされる時間を一層短縮することが可能となる。

ｃ）また、前記ポリシークラスタを用いることによって、ポリシー群と該ポリシーのパラメータへの割り当て規則とを一括して取得でき、さらにポリシークラスタ全体が交渉済みであることを、サービス層３は一度の交渉で容易に確認することができる。さらにポリシークラスタ内の前記署名情報をサービス層３が検証することにより、不正なポリシークラスタや、人為的ミス、通信エラー等の発生を検出でき、信頼性を一層向上させることが可能となる。

【００３０】

【発明の実施の形態】

図１は本発明に基づく分散環境型のコンピュータシステムの基本構成を示す図（その１）、

図２は同図（その２）である。

なお全図を通じて同様の構成要素には同一の参照番号または記号を付して示す。

【００３１】

前述のとおり、図示する２つのコンピュータシステムのうちアプリケーション１を扱うコンピュータシステム（図１）を代表として以下の説明を行う。

図１に示すコンピュータシステムは、図１４および図１５に示すコンピュータシステムと基本的に同様である。すなわち、

アプリケーション１に基づいて一連のメッセージを送受信するメッセージ送受信手段１０と、各前記メッセージに対して特定の制御または指示を与えるためのポリシーに従って、アプリケーション１に対し特定の付加的サービスを提供するサービス層３と、種々のポリシーを保持して一括管理し、サービス層３からの取得の要求に応じて、メッセージに対応するポリシーを供給するポリシー管理装置７と、サービス層３により、ポリシーに従ってサービスが付加されたメッセージを、相手方アプリケーション２との間でやりとりする通信層５と、を備えるコンピュータシステムである。

【００３２】

このようなコンピュータシステムにおいて、本発明の特徴の１つをなすのは、サービス層３内の解析手段３０および要求手段３１である。

解析手段３０は、各メッセージを特定するために各該メッセージに記述されるパラメータを、比較的長時間にわたって変化しない静的パラメータと比較的短時間で変化する動的パラメータとに区分して、各該メッセージより抽出する。

【００３３】

また要求手段３１は、抽出された静的パラメータを用いて、ポリシー管理装置７に対し、該静的パラメータに割り当てられたポリシー群の取得を要求する。

このように要求手段３１から静的パラメータを用いてポリシー群の取得の要求を受けるポリシー管理装置７においては、その要求を受けたとき、ポリシークラスタを生成して要求手段３１に返送するための応答機能部７１を有する。ここに、該ポリシークラスタは、静的パラメータと種々変化する各動的パラメータとを合成してなる全体パラメータの各々に対応するポリシー群と、その全体パラメータの各々に対するポリシー群の各々の割り当てを示すポリシー割り当て規則と、を少なくとも含んで構成される（図５および図６参照）。

【００３４】

このように応答機能部７１から返送されたポリシークラスタを取得する要求手段３１には、ポリシーキャッシュ機能部（３５）が設けられている。このポリシーキャッシュ機能部３５は、ポリシー管理装置７から返送された上記のポリシークラスタを、読み出し自在に、一時的に保存し、メッセージの送受信開始後は、

送信した全体パラメータに割り当てられたポリシークラスタがこのポリシーキャッシュ機能部３５に保存されているときはここから当該ポリシーを取得する。

【００３５】

このポリシーキャッシュ機能部３５内にはまた、交渉済みフラグ領域が設けられる（図７参照）。この交渉済みフラグは、相手方アプリケーション２をサポートする相手方サービス層４との間で事前に交渉して、両者間で適用すべきポリシーについて合意したとき、合意があったことを表示するためのフラグである。

上記の交渉済みフラグに関連するものとして交渉済みタグも採用されている（図４参照）。すなわち、ポリシー管理装置７は、相手方アプリケーション２をサポートする相手方ポリシー管理装置８との間で事前に交渉して、両者間で適用すべきポリシーについて合意したとき、合意があったことを表示するための交渉済みタグをポリシークラスタ内に記録する。またポリシー管理装置７は、ポリシークラスタの内容が正当であることを保証するための署名（図４参照）を生成する署名機能部７３も有している。

【００３６】

上記の交渉済みフラグに関連するものとして交渉機能部３６がある。すなわち、要求手段３１は、ポリシー管理装置７からポリシークラスタを取得した際に、該ポリシークラスタ内に表示された交渉済みタグを用いて相手方サービス層４との間で事前に該交渉済みタグの正当性を相互に確認し合う交渉機能部３６を有している。ここに、交渉機能部３６はポリシークラスタに含まれる複数のポリシーを一括してその交渉を実行する。

【００３７】

要求手段３１は、前記の署名機能部７３に対応させて、ポリシー管理装置７からポリシークラスタを取得した際に、該ポリシークラスタ内に表示された前述の署名が正当であることを検証するための署名検証機能部３９を有する。

上述したコンピュータシステムの理解を一層深めるために、上述した〔パラメータ〕、〔ポリシークラスタ〕および〔ポリシーキャッシュ機能部〕について以下に詳しく説明する。

〔パラメータ〕

本発明ではパラメータは複数の項目からなるものと仮定しており、またそれは多くの場合に成立する仮定である。

【００３８】

多くの利用形態においては、ポリシーを取得するためのパラメータのうち短時間で変化するのは一部の項目である。前記のＣＯＲＢＡの例で言えば、通信の相手方アプリケーション２のうち呼び出すクラス名（あるいはインタフェース名）や呼び出すメソッド名（あるいはオペレーション名）、与えられる引数リストなどは比較的短時間でめまぐるしく変化する。

【００３９】

これに対して、通信している両ホストの名前（識別子）やアプリケーションを利用しているユーザ名等は比較的長時間にわたって変化しない。これを図３を参照して説明する。

図３は本発明に基づく、パラメータの分割について説明するための図である。

本図に示すように、パラメータ（全体パラメータ）１００を、長時間にわたって変化しにくい項目を静的パラメータ１０１、短時間で変化しやすい項目を動的パラメータ１０２、とに区分する。別の言い方をすれば、実際にサービス層３がメッセージを受け取るまで決定できない項目を動的パラメータと定義し、メッセージを受け取る以前にサービス層が決定しうる項目を静的パラメータと定義することもできる。

【００４０】

動的パラメータ１０２は解析手段３０が動的パラメータ解析機能部３７によって、メッセージから抽出する。

一方、静的パラメータ１０１は、解析手段３０が具備する静的パラメータ解析機能部３８によって抽出する。この静的パラメータ１０１は長時間にわたって変化しないから、全体パラメータ１００のうち、静的パラメータ１０１を固定して、動的パラメータ１０２のみが変化した場合に必要となるポリシー群の一部（または全部）を限定することができる。

〔ポリシークラスタ〕

特定のポリシー群をポリシー管理装置７（８）からサービス層３（４）へ受け

渡す際には、複数のポリシー群を一括して渡すことが望まれる。このために、それらのポリシー群に関してどのポリシーをどのような場合に（すなわちどの動的パラメータの値のときに）適用すべきかを定めた割り当て規則も渡すようにする。本発明ではこれらをひとまとめにした前述のポリシークラスタを導入する。

【００４１】

図４は本発明に基づくポリシークラスタの構成を示す図（その１）、

図５は同図（その２）である。

ポリシー管理装置７にて生成されるポリシークラスタは、ポリシーリスト１１３とポリシー割り当て規則リスト１１２、交渉済みタグ１１１、その他の補助情報（図の例では発行者情報１１０）、およびそれらに対して施したディジタル署名１１４の情報を含む。なおディジタル署名とは、ある種の演算によってあるデータから作成され、そのデータの内容の不変性や出所をあとから検証することのできる暗号学的手法であり、ＲＳＡ（Rivest, Shamir, Adleman)演算アルゴリズムによるものが広く知られている。

【００４２】

図４の例では発行者名１１０は任意の情報であるが、署名１１４で出所を示す場合には署名を施す者を指す名前や識別子となる。

交渉済みタグ１１１も任意の情報であるが、この値の定め方については後述する。

次に、ポリシー割り当て規則１１２のリストは、パラメータの値とポリシー名との組による、パラメータ（全体パラメータ）に対するポリシーの割り当て規則を列挙したものである。なお静的パラメータによって取得されたポリシークラスタの場合にはこれらのパラメータの値はすべて指定された同じ静的パラメータ部分を持つのが普通である。

【００４３】

ポリシーリスト１１３は、ポリシー割り当て規則１１２のリストにおいて指示されたポリシーを列挙したものである。

また署名１１４は、予め定めた署名方式によって、署名１１４の欄を除くポリシークラスタの全データに対して施されるディジタル署名である。

〔ポリシーキャッシュ機能部〕

図６は本発明に基づくポリシーキャッシュ機能部を示す図（その１）、

図７は同図（その２）である。

【００４４】

ポリシークラスタ（図４、図５）の形で一括してサービス層３（４）が取得したポリシー群は（ポリシー単独のこともある）、適切な過程を経てポリシーキャッシュ機能部３５（４５）に一時的に保存することができる。

ポリシーキャッシュ機能部３５は、ポリシーを格納するキャッシュメモリ１２２と、ポリシーを格納した格納位置を記録するポリシーキャッシュテーブル１２１と、これらのメモリやテーブルを用いてデータの書き込み、読み出し、検索等を行うキャッシュ制御部１２３と、からなる。

【００４５】

このポリシーキャッシュ機能部３５について特徴的なのは、

（ｉ）キャッシュテーブルが、パラメータ（全体パラメータ）をキーとしてポリシー名を検索するための割り当て規則キャッシュテーブル１２０と、ポリシー名をキーとしてポリシー格納位置を検索するためのポリシーキャッシュテーブル１２１の２つから構成されること、および

（ii）割り当て規則キャッシュテーブル１２０には個々のテーブル項目が指すポリシーが交渉済みであるか否かを記録するための交渉済みフラグ１２５が付与されていること、である。このポリシーキャッシュテーブル１２１の各項目は、ポリシー割り当て規則と同様の意味を持っている。

【００４６】

なお図７の例では、キャッシュテーブル１２０と１２１の双方に、キャッシュ有効期限１２４および１２６の情報がそれぞれ付与されている。ただしこの情報は必要に応じて付加する。

ここで本発明に係る、サービス層３（４）、キャッシュ機能部３５（４５）およびポリシー管理装置７（８）の各々について、その特徴的な構成をまとめて掲記し、そして最後に、図１および図２に示すコンピュータシステム全体の処理の流れを、図８～図１１を参照して、説明する。

〔サービス層〕

まずサービス層３について見るとこれは、アプリケーション１に基づいて送受信される一連のメッセージに対し、外部のポリシー管理装置７と連係しながら、ポリシーに従って特定の付加的サービスを提供するサービス層であって、このサービス層３は、各メッセージを特定するために各メッセージに記述されるパラメータを、比較的長時間にわたって変化しない静的パラメータ１０１と比較的短時間で変化する動的パラメータ１０２とに区分して、各メッセージより抽出する解析手段３０と、抽出された静的パラメータ１０１を用いて、ポリシー管理装置７に対し、この静的パラメータ１０１に割り当てられたポリシー群の取得を要求する要求手段３１と、を有する。

【００４７】

またポリシーに従った付加的サービスを実行する制御手段３２をさらに有する。

また上記の解析手段３０は、静的パラメータ１０１を抽出する静的パラメータ解析機能部３７と動的パラメータ１０２を抽出する動的パラメータ解析機能部３８と、からなる。

【００４８】

一方要求手段３１は、相手方アプリケーション２に送信すべきメッセージに記述される静的パラメータ１０１を用いて、ポリシー管理装置７から静的パラメータ１０１に割り当てられたポリシーの群を取得するポリシー取得機能部３４を有する。

さらにこの要求手段３１は、ポリシー取得機能部３４により取得したポリシーの群を、読み出し自在に、一時的に保存するポリシーキャッシュ機能部３５を有する。

【００４９】

さらにまたその要求手段３１は、ポリシー管理装置７からまたはポリシーキャッシュ機能部３５から取得したポリシーの群の各ポリシーに関し、相手方アプリケーション２をサポートする相手方サービス層４との間で適用すべきポリシーについて、両者（３，４）間で合意するための交渉を行う交渉機能部３６を有する

【００５０】

またその要求手段３１は、ポリシー管理装置７からまたはポリシーキャッシュ機能部３５から取得したポリシーの群に対して記載された署名１１４が正当であることを検証するための署名検証機能部３９を有する。

〔ポリシーキャッシュ機能部〕

次にポリシーキャッシュ機能部３５について見るとこれは、アプリケーション１に基づいて送受信される一連のメッセージに対し、外部のポリシー管理装置７と連係しながら、ポリシーに従って特定の付加的サービスを提供するサービス層３内に設けられるポリシーキャッシュ機能部であって、このポリシーキャッシュ機能部３５は、各メッセージに対して特定の制御または指示を与えるための１または複数のポリシーを、ポリシー管理装置７から取得して一時的に格納するキャッシュメモリ１２２と、ポリシーを格納したキャッシュメモリ１２２内の格納位置を各ポリシー対応に記録するポリシーキャッシュテーブル１２１と、各メッセージを特定するために各メッセージに記述されるパラメータの各々に対するポリシーの割り当て規則を定める割り当て規則キャッシュテーブル１２０と、を有する。

【００５１】

この割り当て規則キャッシュテーブル１２０は、メッセージを送受信する相手方アプリケーション２をサポートするサービス層４との間で事前に交渉して、両者（３，４）間で適用すべきポリシーについて合意したとき、この割り当て規則キャッシュテーブル１２０内に記録された各ポリシーについて合意があったことを表示するための交渉済みフラグ１２５の領域を含む。

〔ポリシー管理装置〕

最後にポリシー管理装置７について見るとこれは、アプリケーション１に基づいて送受信される一連のメッセージに対し特定の付加的サービスを提供するサービス層３と連係し、各メッセージに対して特定の制御または指示を与えるための１または複数のポリシーをこのサービス層３に供給するためのポリシー管理装置であって、このポリシー管理装置７は、サービス層３にて、各メッセージを特定

するために各メッセージに記述されるパラメータを、比較的長時間にわたって変化しない静的パラメータ１０１と比較的短時間で変化する動的パラメータ１０２とに区分して得たパラメータのうちこの静的パラメータ１０１をもって、そのサービス層３より、ポリシーの取得が要求されたとき、ポリシークラスタ（図４、図５）を生成してこのサービス層３に返送する応答機能部７１を有する。ここに、そのポリシークラスタは、静的パラメータ１０１と種々変化する各動的パラメータ１０２とを合成してなる全体パラメータ（図３）の各々に対応するポリシー群と、該全体パラメータの各々に対するポリシー群の各々の割り当てを示すポリシー割り当て規則１１２と、を少なくとも含んで構成される。

【００５２】

一方、ポリシー管理装置７は、メッセージの送受信を行う相手方アプリケーション２をサポートする相手方ポリシー管理装置８との間で事前に交渉して、両者（７，８）間で適用すべきポリシーについて合意したとき、合意があったことを、ポリシークラスタ（図４、図５）内において記録するための交渉済みタグ１１１を生成する事前交渉機能部７３を有すると共に、さらに好ましくは、ポリシークラスタの内容が正当であることを保証するための署名１１４を生成する署名機能部７３を有する。

【００５３】

最後に、図１および図２に示す本発明に係るコンピュータシステム全体の処理の流れをフローチャートを参照して説明する。

図８はポリシークラスタを事前取得する処理を示すフローチャート（その１）

図９は同フローチャート（その２）である。また

図１０はメッセージ通信時の処理を示すフローチャート（その１）、

図１１は同フローチャート（その２）である。

【００５４】

まず図８および図９を参照して説明する。

前述した図１６および図１７に示すフローチャートによれば、アプリケーション１のメッセージ送受手段１０がメッセージを送信する時点からサービス層３の

動作が始まり、メッセージ解析、ポリシー取得とポリシーキャッシュおよびポリシーによる制御の後、メッセージを通信する。

【００５５】

これに対し本発明に基づく処理においては、事前にポリシークラスタを取得する動作とメッセージ通信時にポリシーを取得する動作の２つに分けられる。

〔ポリシークラスタの事前取得〕

図８および図９は、ポリシークラスタを事前に取得する際の処理の流れの例を示すフローチャートである。なお、この事前取得の処理がどのような契機で始まるかについては本発明では特に指定しないが、例えば、アプリケーション１を起動した時点、アプリケーション１にユーザがログインして使用を開始する時点、アプリケーション１から最初のメッセージが送信された時点、等が典型的な開始契機の例として考えられる。

【００５６】

上記の契機により処理が開始されると、サービス層３は解析手段３０が持つ静的パラメータ解析機能部３７により、静的パラメータ１０１を抽出する（Ｓ２１）。静的パラメータ解析機能部が、静的パラメータ（例えばホスト名、ユーザ名等）を抽出する方法は、利用する静的パラメータの種類や実装形態に依存する。例えば、ハードウェアに問い合わせる、オペレーティングシステムや他のソフトウェアに問い合わせる、環境変数から得る、アプリケーションに問い合わせる、等の方法を挙げることができる。このようにして得られた静的パラメータは、例えば解析手段３０が、適切な契機や手段によって消されたり上書きされるまで記憶しておくことができる。この場合、以降で動的パラメータ１０２を抽出するたびに、静的パラメータと動的パラメータを自動的に連結して、１つの全体パラメータ１００とすることもできる。

【００５７】

このようにして得られた静的パラメータ１０１を用い、要求手段３１はポリシー取得機能部３４を用いて、適切なポリシークラスタをポリシー管理装置７へ問い合わせる（Ｓ２２）。ポリシー管理装置７はこの静的オペレータ１０１に対応したポリシー群の一部（または全部）を含んだポリシークラスタ（図４および図

５）を返送する。このポリシークラスはポリシー管理装置７が、上記機能部３４から問い合わせを受けてから生成しても構わないが、あらかじめ作成して保持しておくことが望ましい。特に交渉済みタグ１１１（図４および図５）を利用する際にはそうである。なおポリシークラスタの生成については、後にさらに詳しく説明する。

【００５８】

サービス層３は、ポリシークラスタを受け取ると（Ｓ２３のＹｅｓ）、署名１１４の検証、ポリシークラスタの一括交渉を行うことができる。ただしこのときにポリシークラスタに署名１１４があるか否か判定し（Ｓ２５）、その後、ポリシークラスタを構成するポリシーリスト１１３のポリシー群とポリシー割り当て規則１１２をポリシーキャッシュ機能部３５へ一時保存する。

【００５９】

署名１１４の検証は要求手段３０が持つ署名検証機能部３９によって行う（Ｓ２７）。前述したＲＳＡ演算アルゴリズムの例であれば、ポリシークラスタの発行者（署名者）１１０の公開鍵を用いて、このポリシークラスタが確かに発行者が作成したものかどうか、さらに、作成されてから改変がされていないか、確認する。もし署名が不正であれば（Ｓ２８のＮｏ）、署名が不正であった場合のエラー処理を行う（Ｓ２９）。

【００６０】

このエラー処理の例としては、ユーザに報告する、ログに記録する、サービス層３およびアプリケーション１の動作を停止する、署名がなかった場合と同様に署名を無視する、等が考えられる。

ポリシークラスタの一括交渉は要求手段３０が持つ交渉機能部３６によって行う。もしポリシークラスタに交渉済みタグ１１１がついており、このタグ１１１を利用するならば、交渉機能部３６は、通信の相手方サービス層４の交渉機能部４６と連絡をとり、交渉済みタグ１１１が正当であるか、一致しているか、等を確認する。もしこのタグが正しければ、ポリシークラスタ全体が交渉済みと見なされる。一方、交渉済みタグ１１１を利用しないならば、交渉機能部３６は、ポリシークラスタに含まれるポリシー割り当て規則１１２の全部（または一部）を

通信の相手方サービス層４の交渉機能部４６との間で照合し、該規則１１２が双方で一致していれば交渉済みと見なす（Ｓ３０）。

【００６１】

なお、図には示されていないが、上記の交渉を受け付ける通信の相手方要求手段４０も適切な手段を用いてポリシークラスタを取得する。その方法としては、あらかじめ前記の方法で静的パラメータを抽出しておき、静的パラメータを用いてポリシー管理装置８からポリシークラスタを取得することが例として挙げられる。また交渉機能部同士（３６，４６）で、パラメータの一部を交換して不足する情報を補うことも可能である。

【００６２】

その後、要求手段３０はポリシークラスタを分解してポリシーキャッシュ機能部３５に保存する（通信の相手方要求手段４０についても同様）（Ｓ３１）。すなわち個々のポリシー割り当て規則１１２に従って、指定されたポリシーを取り出し、キャッシュテーブル１２０（１２１）に正しく記録しながら、キャッシュメモリ１２２に保存していく。

【００６３】

このときそのポリシーが交渉済みと見なされている場合は、対応する割り当て規則キャッシュテーブル１２０（図６および図７）の中に交渉済みフラグ１２５を立てる（図７の例では該フラグ１２５をｙｅｓとする）。

〔ポリシークラスタの事前生成と事前交渉〕

既に述べたように、ポリシークラスタは事前に生成し交渉しておくことができる。ある静的パラメータ１０１の値に対してポリシークラスタを生成するには、ポリシー管理装置７は、ポリシー割り当て規則群（図示せず）から、該静的パラメータ値に対応する規則群を全部（または一部）抜き出し、それら規則群とそれら規則群が割り当てているポリシーとを、ポリシークラスタに格納する。これに補助情報（例えば発行者名）や交渉済みタグを加えてもよい。もし署名を付与するならば、最後にこれらポリシーと補助情報の全体に対して署名を施す。

【００６４】

上記の交渉済みタグは任意の情報であり、交渉を成立させた他のポリシー管理

装置との間で矛盾のない値を与える。「矛盾のない」とは、単純には同じ値とすることでもよいが、容易には衝突が起こらないような値を選ぶことが望ましい。例えば、該交渉タグの前半部にはシリアル番号や日時を用い、その後半部には乱数を用いて、両者を連結する、等の方法が挙げられる（図５のＴ参照）。

【００６５】

また相互に異なる値であるが、ディジタル署名等の暗号学的手法を用いて、相互に信用し得る偽造不可能な値を与えることも可能である。当然ながら、前記サービス層３および４の交渉機能部によるポリシークラスタの一括交渉の方法は、当該ポリシークラスタの生成方法に従って決まることになる。

〔メッセージ通信時〕

図１０および図１１は、本発明におけるメッセージ通信時の処理の流れを示す。

【００６６】

アプリケーション１のメッセージ送受手段１０がメッセージを送信し（Ｓ４１）、サービス層３がこのメッセージを受信したならば、サービス層３の解析手段３０は、動的パラメータ解析機能部３８を用いてその受信メッセージを解析し、動的パラメータ１０２を抽出する（Ｓ４２）。例えば、既述のＣＯＲＢＡの場合には、呼び出そうとしているクラス名、メソッド名、引数リスト等が動的パラメータ１０２として得られる。この動的パラメータを、既に取得している静的パラメータ１０１と結合すると、上記受信メッセージに対する全体パラメータ１００となる（Ｓ４２）。

【００６７】

次に、要求手段３１はこの全体パラメータ１００を用いて、ポリシーキャッシュ機能部３５→ポリシー管理装置７、の順に問い合わせ、当該パラメータに割り当てられたポリシーを取得する（Ｓ４３）。

ポリシーキャッシュ機能部３５から得られた場合には（Ｓ４４のＹｅｓ）、割り当て規則キャッシュテーブル１２０を参照して、当該ポリシーが交渉済みであるかどうか（図７）を確認する。

【００６８】

一方、そのポリシーがポリシーキャッシュ機能部３５に見つからず（Ｓ４４のＮｏ）、ポリシー管理装置７から取得した場合には（Ｓ４８，Ｓ４９のＹｅｓ）、この取得したポリシーをポリシーキャッシュ機能部３５に格納することができる。この場合には、当該ポリシーについては交渉済みではないと見なす。

取得したポリシーが交渉済みでなければ（Ｓ４５のＮｏ）、要求手段３１は交渉機能部３６を用いて通信の相手方機能部４６と交渉を行う（Ｓ５３）。単独のポリシーに対する交渉の方法は本発明では特に限定しないが、例えばその交渉の方法については、ポリシー名だけを比較する、ポリシーの指示する制御内容も比較する等が考えられる。

【００６９】

また交渉結果の決め方については、両ポリシーが一致しない場合には交渉不成立とする、ある優先順位に基づいて一方のポリシーを用いるなどの方法が考えられる。いずれにせよ、交渉結果はポリシーキャッシュ機能部３５に交渉済みフラグ１２５として記録する。そして交渉が成立しなかった場合には（Ｓ５３のＮｏ）、任意の交渉不成立時のエラー処理を行う（Ｓ５４）。

【００７０】

一方、交渉済みであるか交渉が成立した場合には（Ｓ５３のＹｅｓ）、そのポリシーは制御手段３２に与えられ、通信に携わるサービス層３および４のそれぞれの制御手段３５および４５が、そのポリシーで指定された制御を行う（Ｓ４６）。既に述べたように、この制御の内容としては、認証、暗号化、署名等のセキュリティ機能が典型的である。しかし本発明はこのセキュリティ機能に限定されることはない。

【００７１】

この制御が終了したならば、当該メッセージは制御手段３２および４２の適切な制御下でそれぞれ通信層５および６を介して伝播され、通信の相手方アプリケーション２がこれを受信する。

以上の説明ではポリシーがキャッシュ機能部３５に見つからなかったり、ポリシーについて交渉済みでなかったりした場合の処理も述べているが、前記のポリシークラスタによる一括取得や一括交渉が適切に行われれば、キャッシュミスと

なったりまた交渉済みでないポリシーに当たることは、最小限の場合に限られる。したがって、ポリシー管理装置７への問い合わせ処理やポリシー毎の交渉の処理を飛ばして、迅速な動作が可能である。

【００７２】

以上詳述した本発明の実施態様は、以下のとおりである。

（付記１）アプリケーションに基づいて一連のメッセージを送受信するメッセージ送受信手段と、

各前記メッセージに対して特定の制御または指示を与えるためのポリシーに従って、前記アプリケーションに対し特定の付加的サービスを提供するサービス層と、

種々の前記ポリシーを保持して一括管理し、前記サービス層からの取得の要求に応じて、前記メッセージに対応する前記ポリシーを供給するポリシー管理装置と、

前記サービス層により、前記ポリシーに従って前記サービスが付加された前記メッセージを、相手方アプリケーションとの間でやりとりする通信層と、を備えるコンピュータシステムにおいて、

前記サービス層内に、

各前記メッセージを特定するために各該メッセージに記述されるパラメータを、比較的長時間にわたって変化しない静的パラメータと比較的短時間で変化する動的パラメータとに区分して、各該メッセージより抽出する解析手段と、

抽出された前記静的パラメータを用いて、前記ポリシー管理装置に対し、該静的パラメータに割り当てられたポリシー群の取得を要求する要求手段と、を形成することを特徴とするコンピュータシステム。

【００７３】

（付記２）前記ポリシー管理装置は、前記要求手段から前記静的パラメータを用いて前記の取得の要求を受けたとき、ポリシークラスタを生成して該要求手段に返送する応答機能部を有し、ここに、該ポリシークラスタは、該静的パラメータと種々変化する各動的パラメータとを合成してなる全体パラメータの各々に対応するポリシー群と、該全体パラメータの各々に対する該ポリシー群の各々の割

り当てを示すポリシー割り当て規則と、を少なくとも含んで構成されることを特徴とする付記１に記載のコンピュータシステム。

【００７４】

（付記３）前記要求手段はポリシーキャッシュ機能部を有し該ポリシーキャッシュ機能部は、前記ポリシー管理装置から返送された前記ポリシークラスタを、読み出し自在に、一時的に保存し、前記メッセージの送受信開始後は、送信した前記全体パラメータに割り当てられた前記ポリシークラスタが該ポリシーキャッシュ機能部に保存されているときはここから当該ポリシーを取得することを特徴とする付記２に記載のコンピュータシステム。

【００７５】

（付記４）前記要求手段は、前記相手方アプリケーションをサポートする相手方サービス層との間で事前に交渉して、両者間で適用すべきポリシーについて合意したとき、合意があったことを表示するための交渉済みフラグ領域を前記ポリシーキャッシュ機能部内に有することを特徴とする付記３に記載のコンピュータシステム。

【００７６】

（付記５）前記ポリシー管理装置は、前記相手方アプリケーションをサポートする相手方ポリシー管理装置との間で事前に交渉して、両者間で適用すべきポリシーについて合意したとき、合意があったことを表示するための交渉済みタグを前記ポリシークラスタ内に記憶することを特徴とする付記４に記載のコンピュータシステム。

【００７７】

（付記６）前記ポリシー管理装置は、前記ポリシークラスタの内容が正当であることを保証するための署名を生成する署名機能部を有することを特徴とする付記２に記載のコンピュータシステム。

（付記７）前記要求手段は、前記ポリシー管理装置から前記ポリシークラスタを取得した際に、該ポリシークラスタ内に表示された前記交渉済みタグを用いて前記相手方サービス層との間で事前に該交渉済みタグの正当性を相互に確認し合う交渉機能部を有し、ここに、該交渉機能部は該ポリシークラスタに含まれる複

数のポリシーを一括してその交渉を実行することを特徴とする付記５に記載のコンピュータシステム。

【００７８】

（付記８）前記要求手段は、前記ポリシー管理装置から前記ポリシークラスタを取得した際に、該ポリシークラスタ内に表示された前記署名が正当であることを検証するための署名検証機能部を有することを特徴とする付記６に記載のコンピュータシステム。

（付記９）アプリケーションに基づいて送受信される一連のメッセージに対し、外部のポリシー管理装置と連係しながら、ポリシーに従って特定の付加的サービスを提供するサービス層であって、

該サービス層は、

各前記メッセージを特定するために各該メッセージに記述されるパラメータを、比較的長時間にわたって変化しない静的パラメータと比較的短時間で変化する動的パラメータとに区分して、各該メッセージより抽出する解析手段と、

抽出された前記静的パラメータを用いて、前記ポリシー管理装置に対し、該静的パラメータに割り当てられたポリシー群の取得を要求する要求手段と、

を有することを特徴とするサービス層。

【００７９】

（付記１０）前記ポリシーに従った前記付加的サービスを実行する制御手段をさらに有することを特徴とする付記９に記載のサービス層。

（付記１１）前記解析手段は、前記静的パラメータを抽出する静的パラメータ解析機能部と前記動的パラメータを抽出する動的パラメータ解析機能部と、からなることを特徴とする付記９に記載のサービス層。

【００８０】

（付記１２）前記要求手段は、相手方アプリケーションに送信すべき前記メッセージに記述される前記静的パラメータを用いて、前記ポリシー管理装置から該静的パラメータに割り当てられたポリシーの群を取得するポリシー取得機能部を有することを特徴とする付記９に記載のサービス層。

（付記１３）前記要求手段は、前記ポリシー取得機能部により取得した前記ポ

リシーの群を、読み出し自在に、一時的に保存するポリシーキャッシュ機能部を有することを特徴とする付記１２に記載のサービス層。

【００８１】

（付記１４）前記要求手段は、前記ポリシー管理装置からまたは前記ポリシーキャッシュ機能部から取得した前記ポリシーの群の各ポリシーに関し、前記相手方アプリケーションをサポートする相手方サービス層との間で適用すべきポリシーについて、両者間で合意するための交渉を行う交渉機能部を有することを特徴とする付記１３に記載のサービス層。

【００８２】

（付記１５）前記要求手段は、前記ポリシー管理装置からまたは前記ポリシーキャッシュ機能部から取得した前記ポリシーの群に対して記載された署名が正当であることを検証するための署名検証機能部を有することを特徴とする付記１３に記載のサービス層。

（付記１６）アプリケーションに基づいて送受信される一連のメッセージに対し、外部のポリシー管理装置と連係しながら、ポリシーに従って特定の付加的サービスを提供するサービス層内に設けられるポリシーキャッシュ機能部であって、

該ポリシーキャッシュ機能部は、

各前記メッセージに対して特定の制御または指示を与えるための１または複数のポリシーを、前記ポリシー管理装置から取得して一時的に格納するキャッシュメモリと、

前記ポリシーを格納した前記キャッシュメモリ内の格納位置を各ポリシー対応に記録するポリシーキャッシュテーブルと、

各前記メッセージを特定するために各該メッセージに記述されるパラメータの各々に対する前記ポリシーの割り当て規則を定める割り当て規則キャッシュテーブルと、

を有することを特徴とするポリシーキャッシュ機能部。

【００８３】

（付記１７）前記割り当て規則キャッシュテーブルは、前記メッセージを送受

信する相手方アプリケーションをサポートするサービス層との間で事前に交渉して、両者間で適用すべきポリシーについて合意したとき、前記割り当て規則キャッシュテーブル内に記録された各前記ポリシーについて合意があったことを表示するための交渉済みフラグ領域を含むことを特徴とする付記１６に記載のポリシーキャッシュ機能部。

【００８４】

（付記１８）アプリケーションに基づいて送受信される一連のメッセージに対し特定の付加的サービスを提供するサービス層と連係し、各前記メッセージに対して特定の制御または指示を与えるための１または複数のポリシーを該サービス層に供給するためのポリシー管理装置であって、

該ポリシー管理装置は、

前記サービス層にて、各前記メッセージを特定するために各該メッセージに記述されるパラメータを、比較的長時間にわたって変化しない静的パラメータと比較的短時間で変化する動的パラメータとに区分して得たパラメータのうち該静的パラメータをもって、該サービス層より、前記ポリシーの取得が要求されたとき、ポリシークラスタを生成して該サービス層に返送する応答機能部を有し、

ここに、該ポリシークラスタは、該静的パラメータと種々変化する各動的パラメータとを合成してなる全体パラメータの各々に対応するポリシー群と、該全体パラメータの各々に対する該ポリシー群の各々の割り当てを示すポリシー割り当て規則と、を少なくとも含んで構成されることを特徴とするポリシー管理装置。

【００８５】

（付記１９）前記メッセージの送受信を行う相手方アプリケーションをサポートする相手方ポリシー管理装置との間で事前に交渉して、両者間で適用すべきポリシーについて合意したとき、合意があったことを、前記ポリシークラスタ内において記録するための交渉済みタグを生成する事前交渉機能部を有することを特徴とする付記１８に記載のポリシー管理装置。

【００８６】

（付記２０）前記ポリシークラスタの内容が正当であることを保証するための署名を生成する署名機能部を有することを特徴とする付記１８に記載のポリシー

管理装置。

【００８７】

【発明の効果】

以上説明したように本発明によれば、分散環境で複数の異なる種類のメッセージを短時間内に通信するような利用形態において生じ易い、メッセージ通信毎のポリシーの問い合わせや通信の相手方との交渉の処理をできる限り不要とすることができる。したがってそのような利用形態における連続したメッセージ通信を、サービス層が高速に処理することが可能となる。

【００８８】

また、不正なポリシー管理装置や人為的ミス、通信エラー等による、ポリシーやポリシーの事前交渉済みの有無に関する情報の不一致を、サービス層が事前に検出することができ、このためコンピュータシステムの信頼性を一層高めることが可能となる。

【図面の簡単な説明】

【図１】

本発明に基づく分散環境型のコンピュータシステムの基本構成を示す図（その１）である。

【図２】

本発明に基づく分散環境型のコンピュータシステムの基本構成を示す図（その２）である。

【図３】

本発明に基づく、パラメータの分割について説明するための図である。

【図４】

本発明に基づくポリシークラスタの構成を示す図（その１）である。

【図５】

本発明に基づくポリシークラスタの構成を示す図（その２）である。

【図６】

本発明に基づくポリシーキャッシュ機能部の構成を示す図（その１）である。

【図７】

本発明に基づくポリシーキャッシュ機能部の構成を示す図（その２）である。

【図８】

ポリシークラスタを事前取得する処理を示すフローチャート（その１）である。

【図９】

ポリシークラスタを事前取得する処理を示すフローチャート（その２）である。

【図１０】

メッセージ通信時の処理を示すフローチャート（その１）である。

【図１１】

メッセージ通信時の処理を示すフローチャート（その２）である。

【図１２】

既に提案されている、分散環境型のコンピュータシステムを示す図（その１）である。

【図１３】

既に提案されている、分散環境型のコンピュータシステムを示す図（その２）である。

【図１４】

本発明の前提をなす分散環境型のコンピュータシステムを示す図（その１）である。

【図１５】

本発明の前提をなす分散環境型のコンピュータシステムを示す図（その２）である。

【図１６】

図１４および図１５に示す本発明の前提をなすコンピュータシステムにおける処理の流れを示すフローチャート（その１）である。

【図１７】

図１４および図１５に示す本発明の前提をなすコンピュータシステムにおける処理の流れを示すフローチャート（その２）である。

【符号の説明】

１，２…アプリケーション

３，４…サービス層

５，６…通信層

７，８…ポリシー管理装置

１０，２０…メッセージ送受信手段

３０，４０…解析手段

３１，４１…要求手段

３２，４２…制御手段

３４，４４…ポリシー取得機能部

３５，４５…ポリシーキャッシュ機能部

３６，４６…交渉機能部

３７，４７…静的パラメータ解析部

３８，４８…動的パラメータ解析部

３９，４９…署名検証機能部

７０，８０…ポリシー記憶領域

７１，８１…応答機能部

７２，８２…事前交渉機能部

７３，８３…署名機能部

１００…全体パラメータ

１０１…静的パラメータ

１０２…動的パラメータ

１１１…交渉済みタグ

１１２…ポリシー割り当て規則

１１３…ポリシーリスト

１１４…署名

１２０…割り当て規則キャッシュテーブル

１２１…ポリシーキャッシュテーブル

１２２…キャッシュメモリ

１２３…キャッシュ制御部

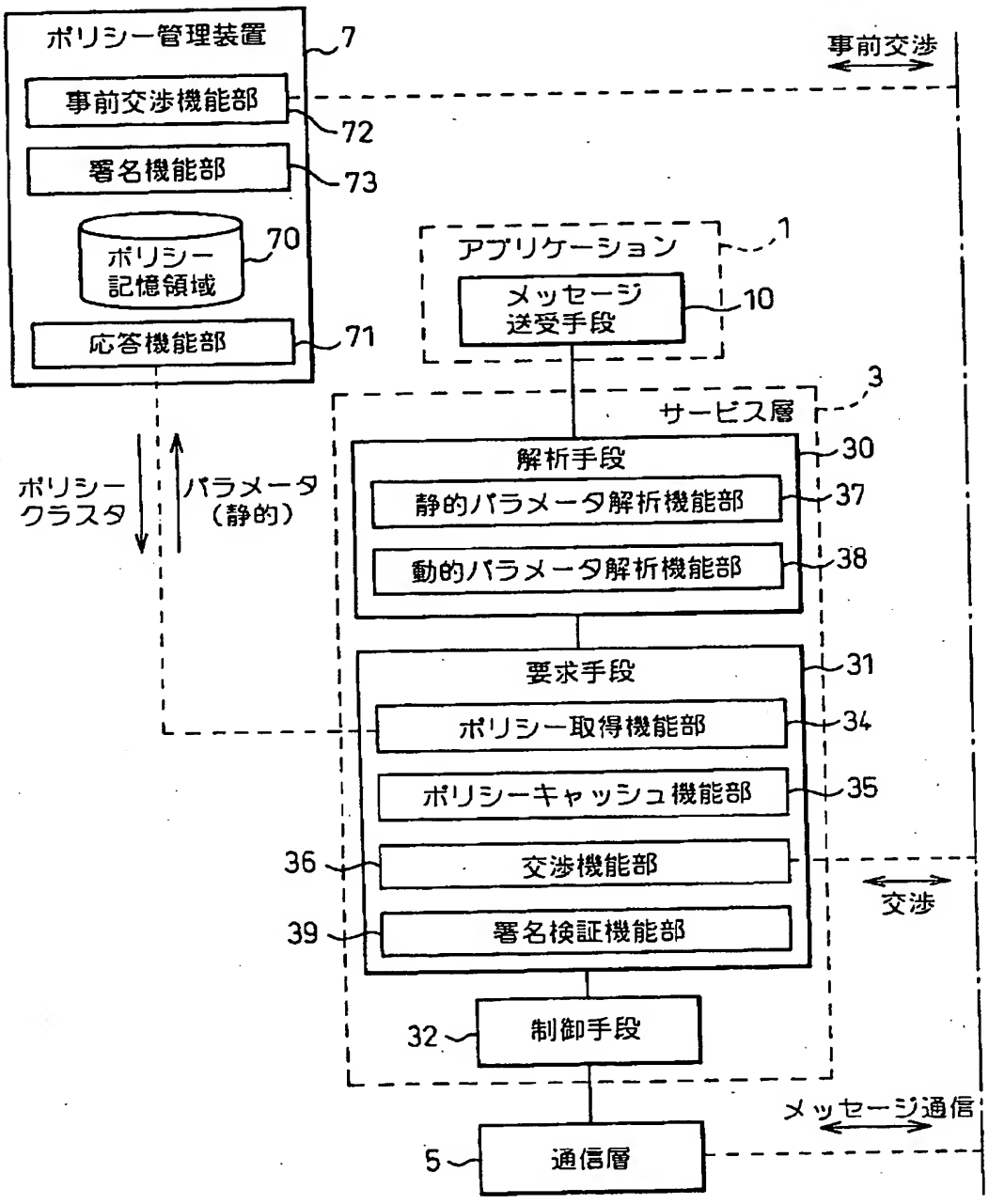
１２４，１２６…キャッシュ有効期限

１２５…交渉済みフラグ

【書類名】　　図面

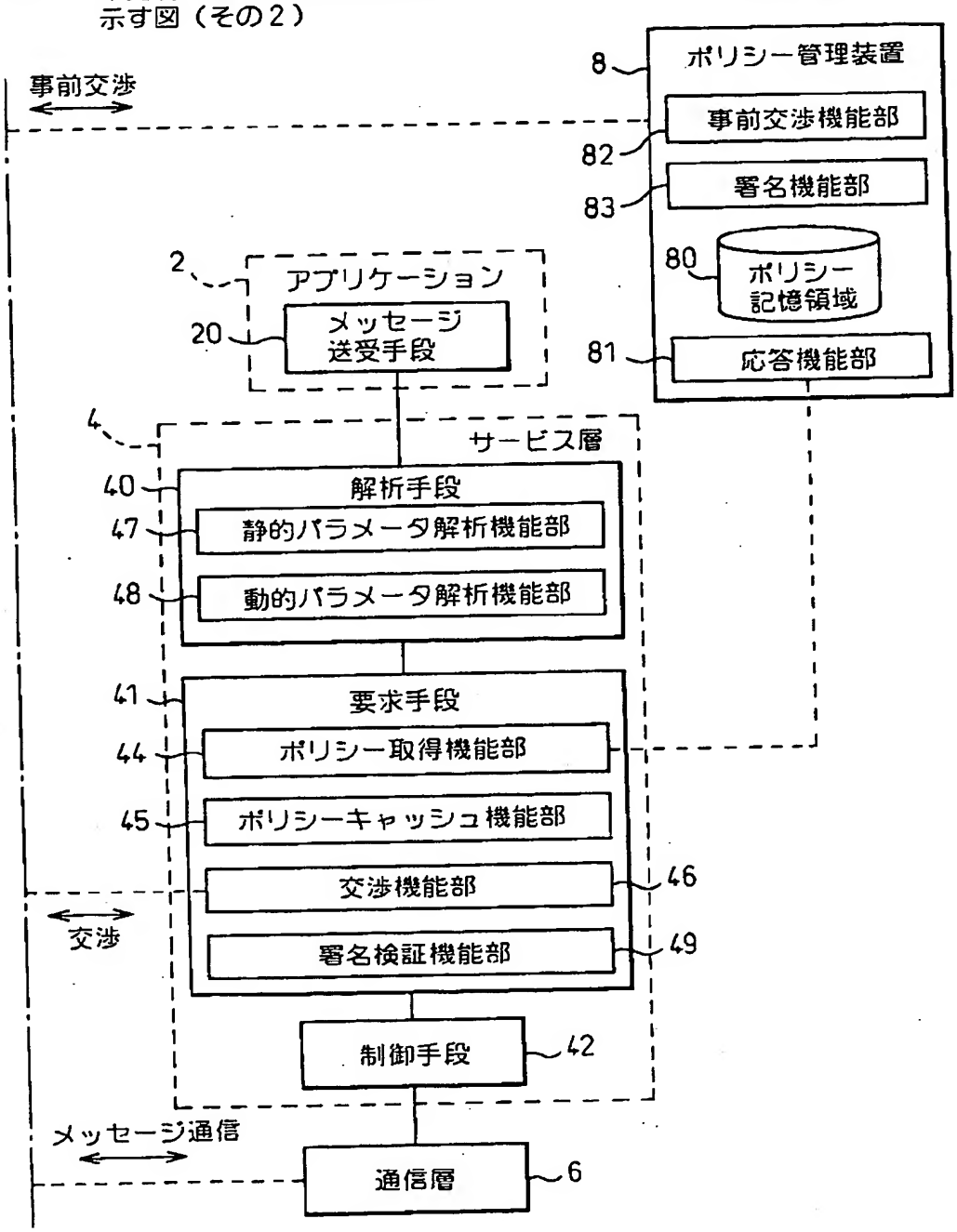
【図１】

図１　本発明に基づく分散環境形のコンピュータシステムの基本構成を示す図（その１）



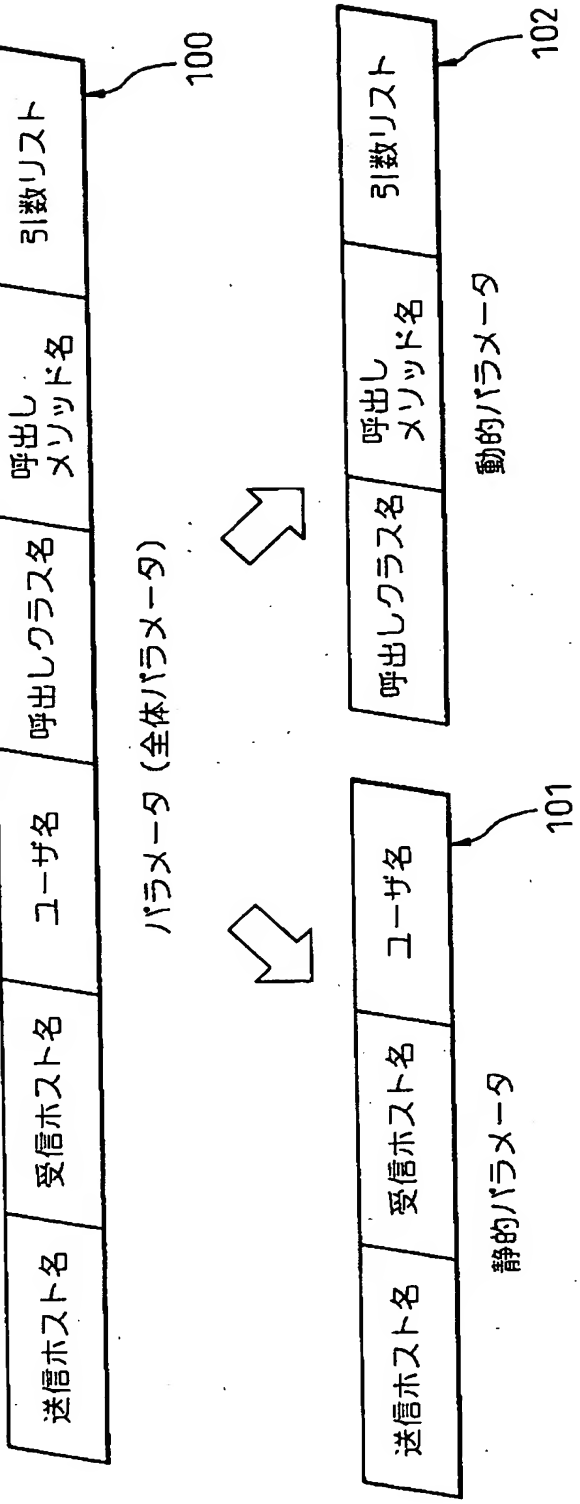
【図２】

図２　本発明に基づく分散環境形のコンピュータシステムの基本構成を示す図（その２）



【図３】

図３

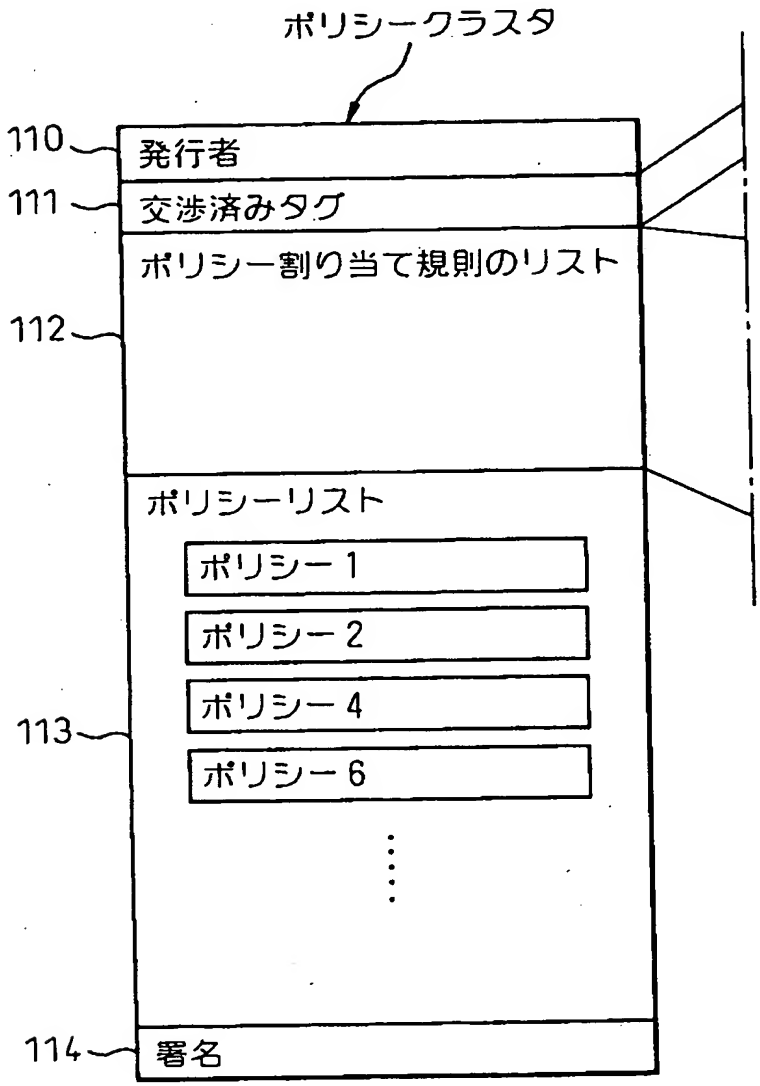


本発明に基づく、パラメータの分割について説明するための図

【図４】

図４

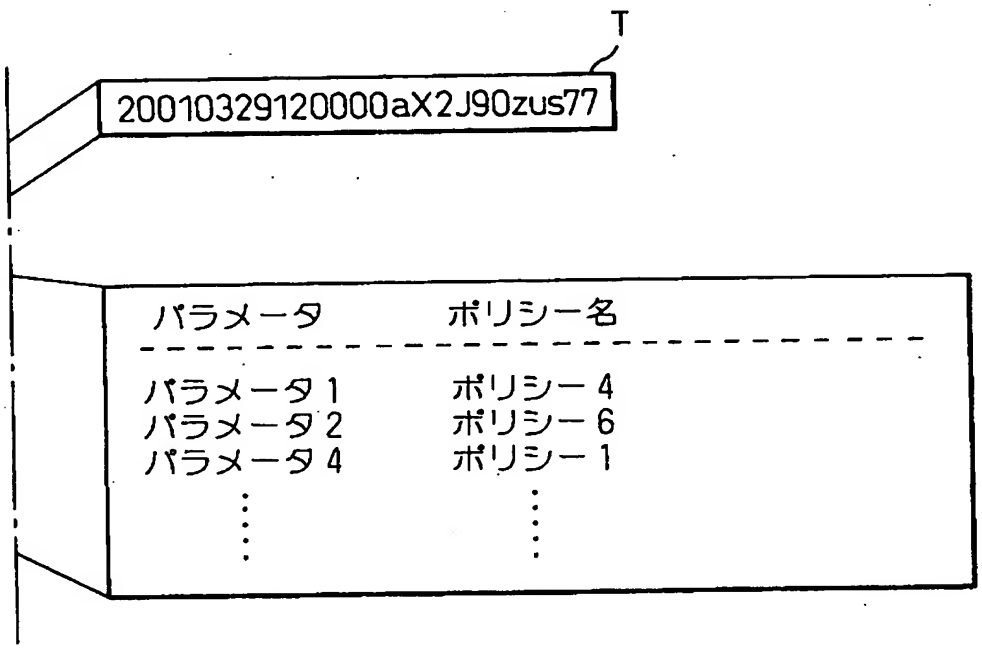
本発明に基づくポリシークラスタの構成を示す図（その１）



【図５】

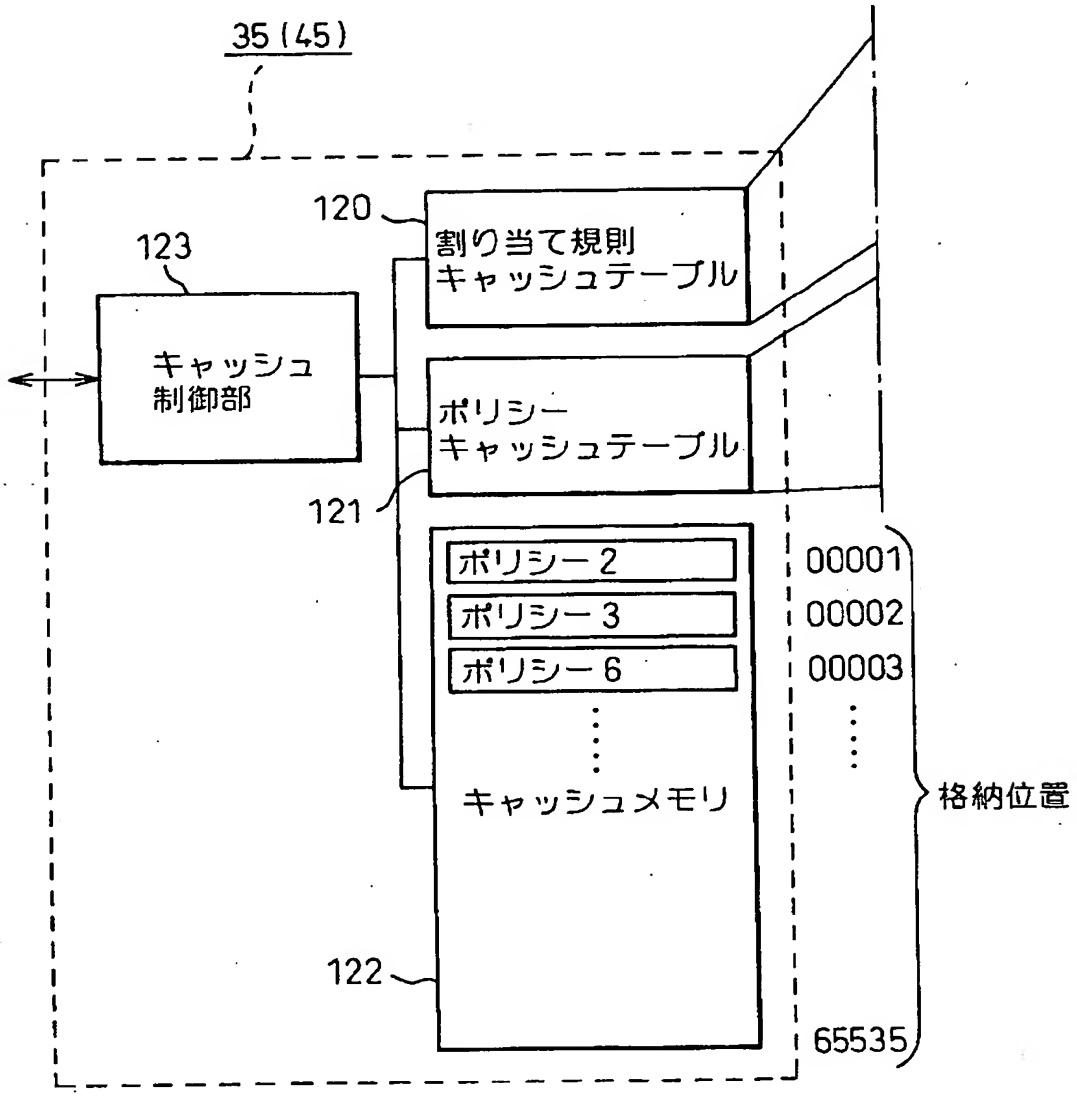
図５

本発明に基づくポリシークラスタの構成を示す図（その２）



【図６】

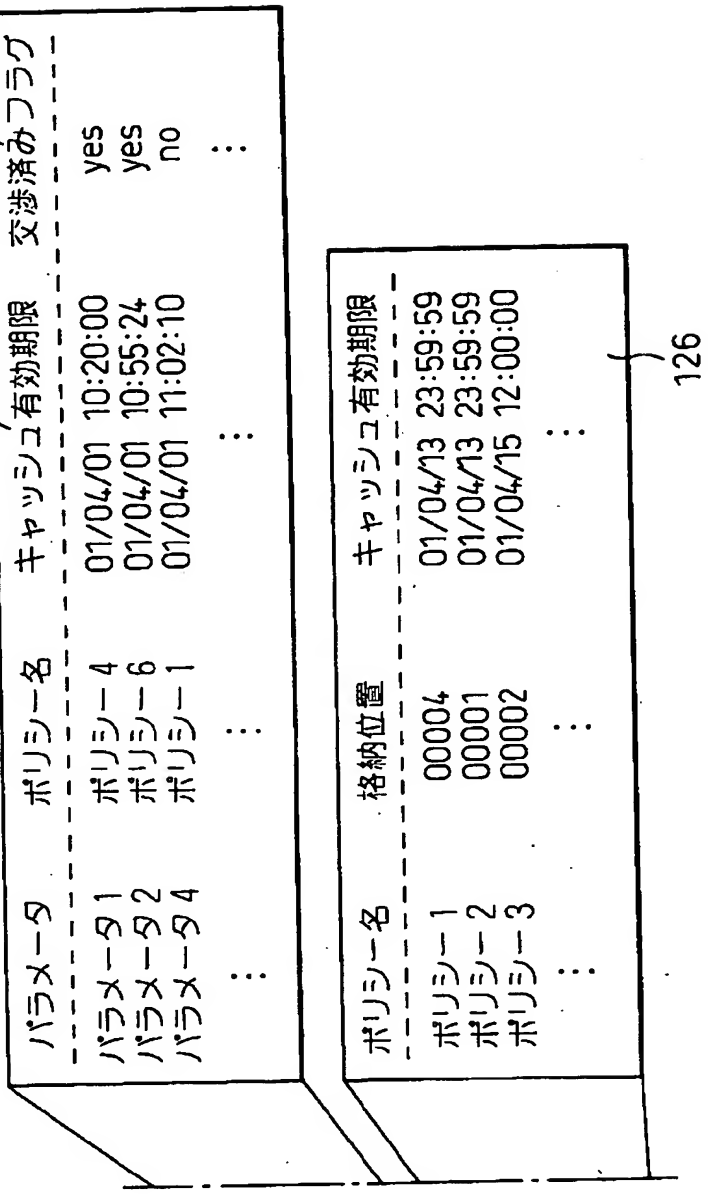
図６
本発明に基づくポリシーキャッシュ機能部の構成を示す図（その１）



【図７】

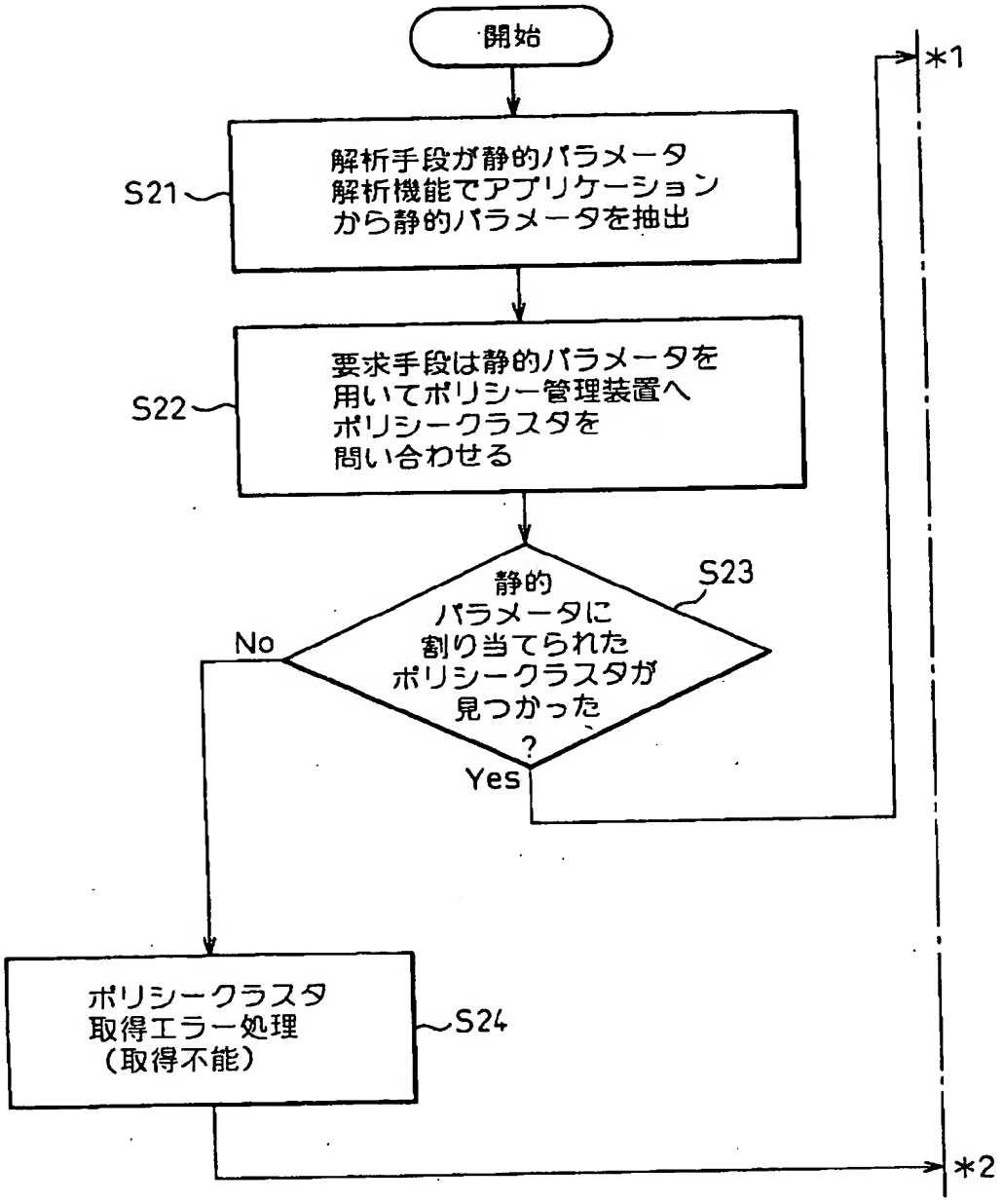
図７

本発明に基づくポリシーキャッシュ機能部の構成を示す図（その２）



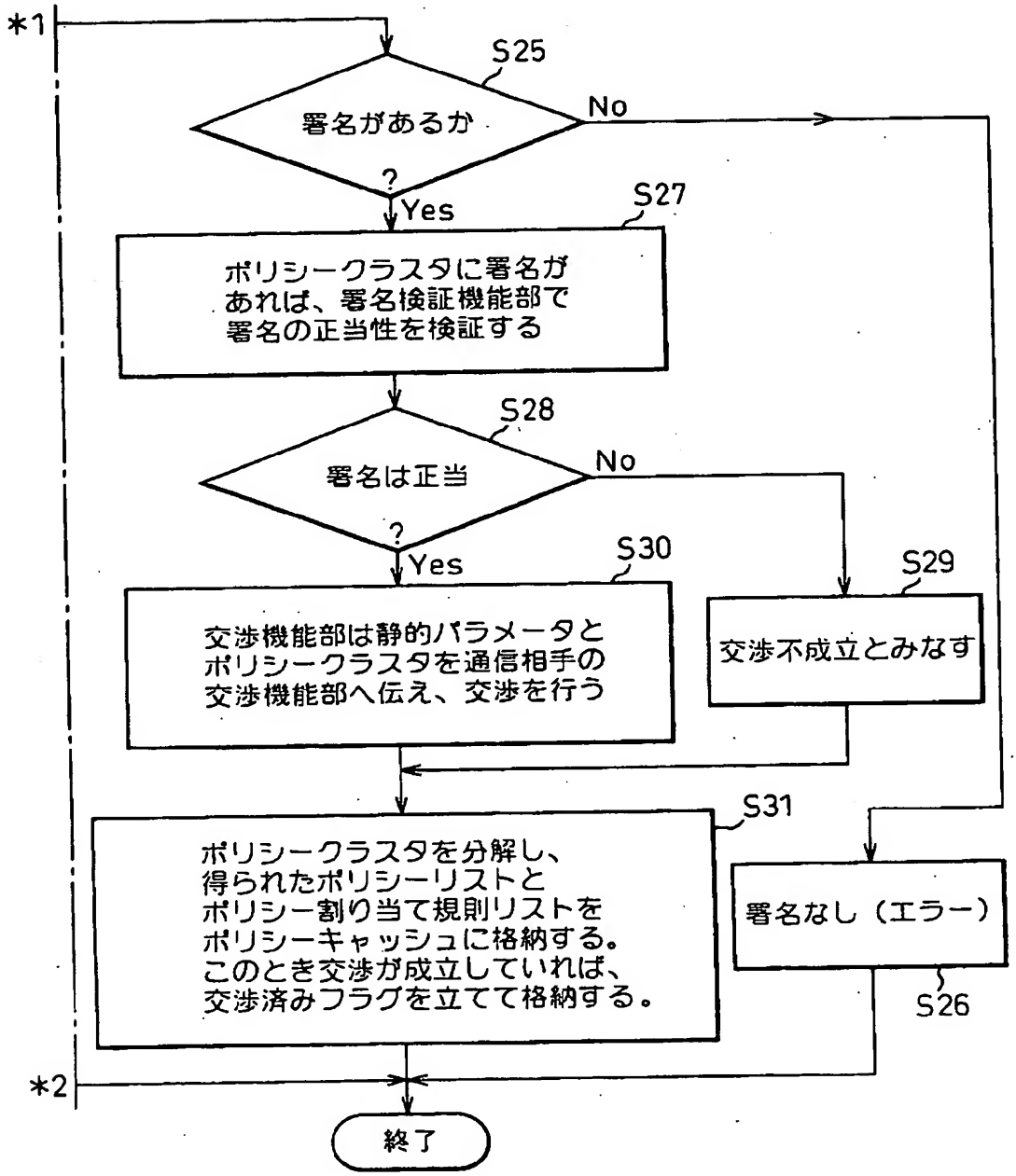
【図８】

図８　ポリシークラスタを事前取得する処理を示すフローチャート（その１）



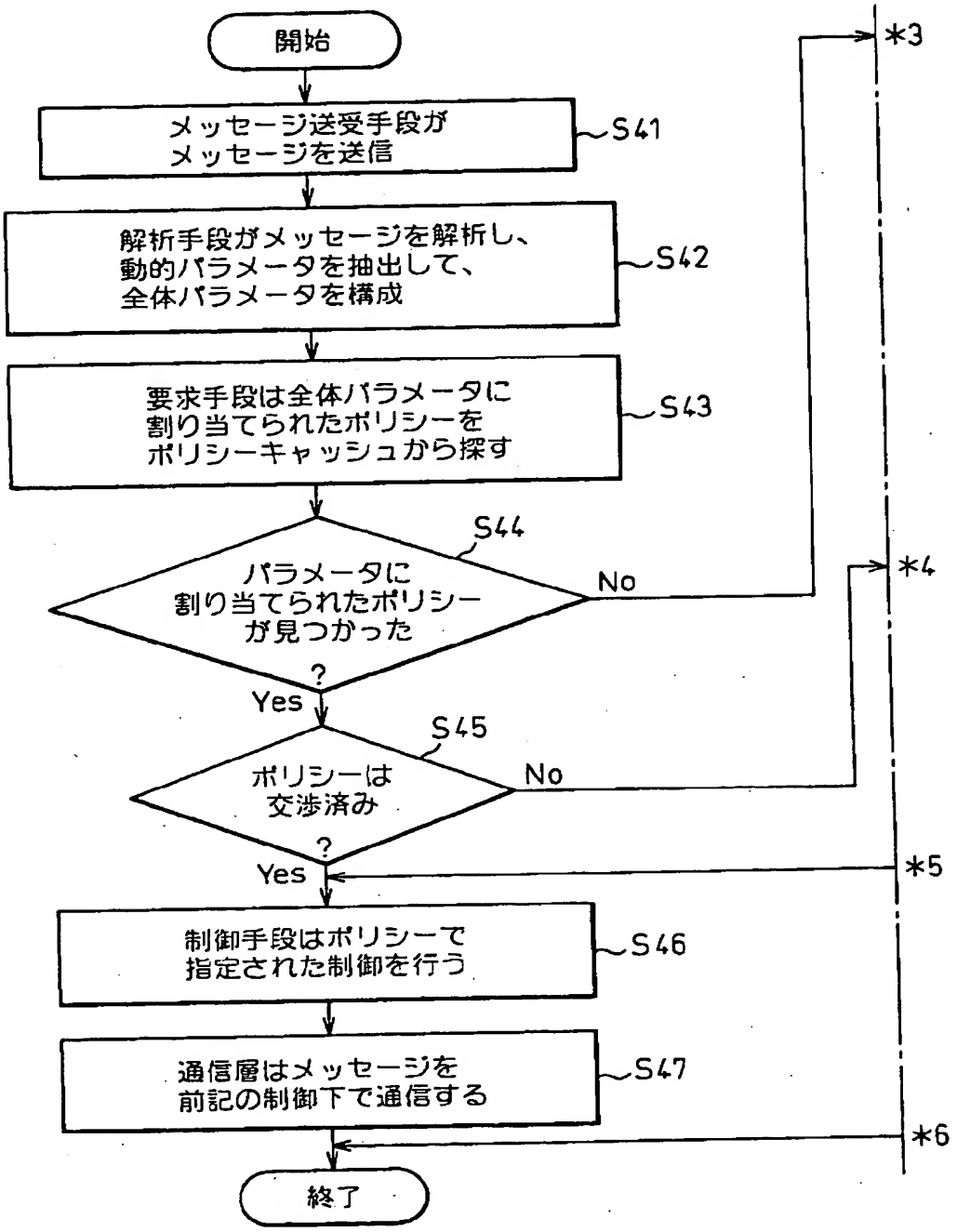
【図９】

図９　ポリシークラスタを事前取得する処理を示すフローチャート（その２）



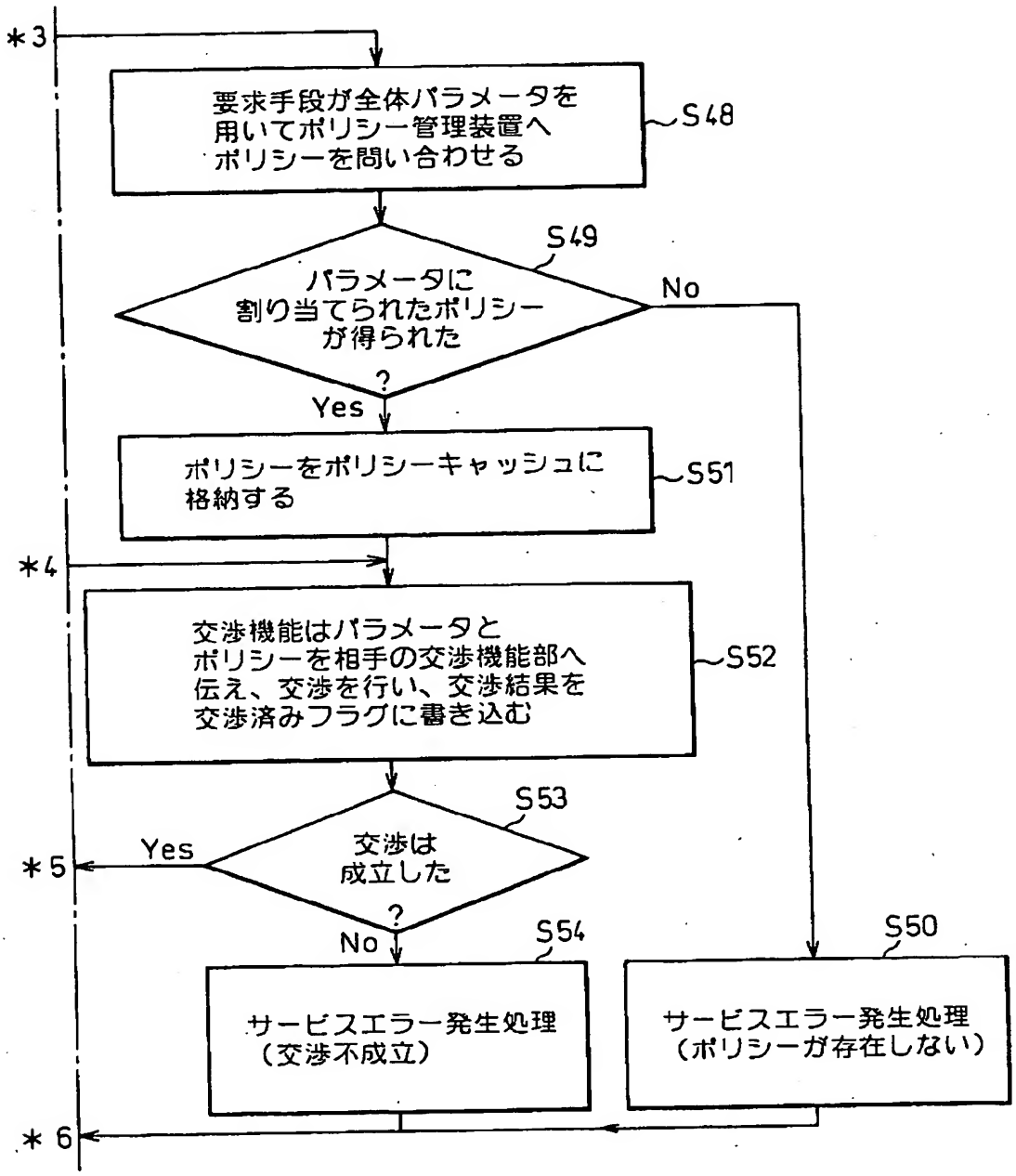
【図１０】

図10　メッセージ通信時の処理を示すフローチャート（その１）



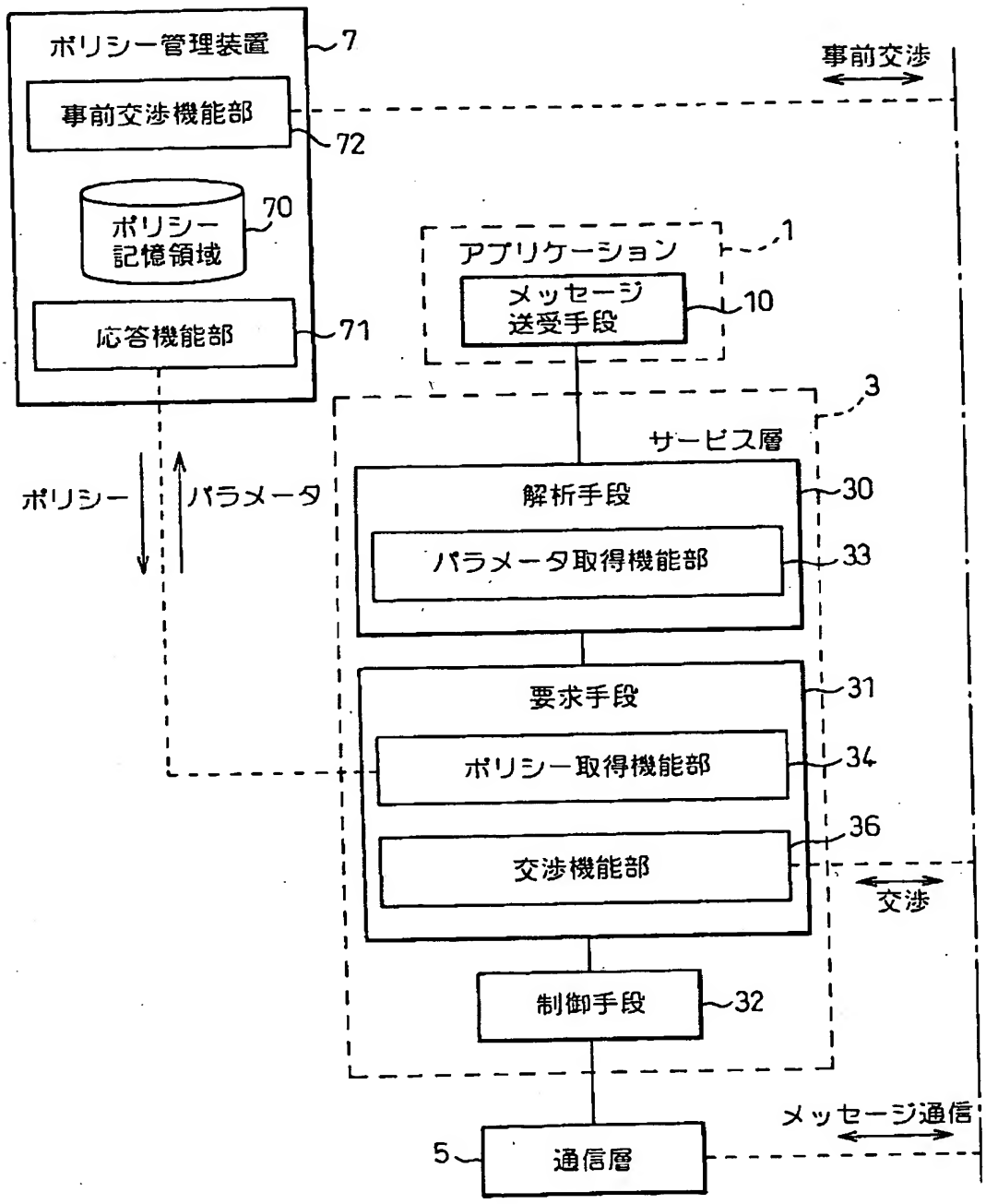
【図１１】

図11　メッセージ通信時の処理を示すフローチャート（その２）



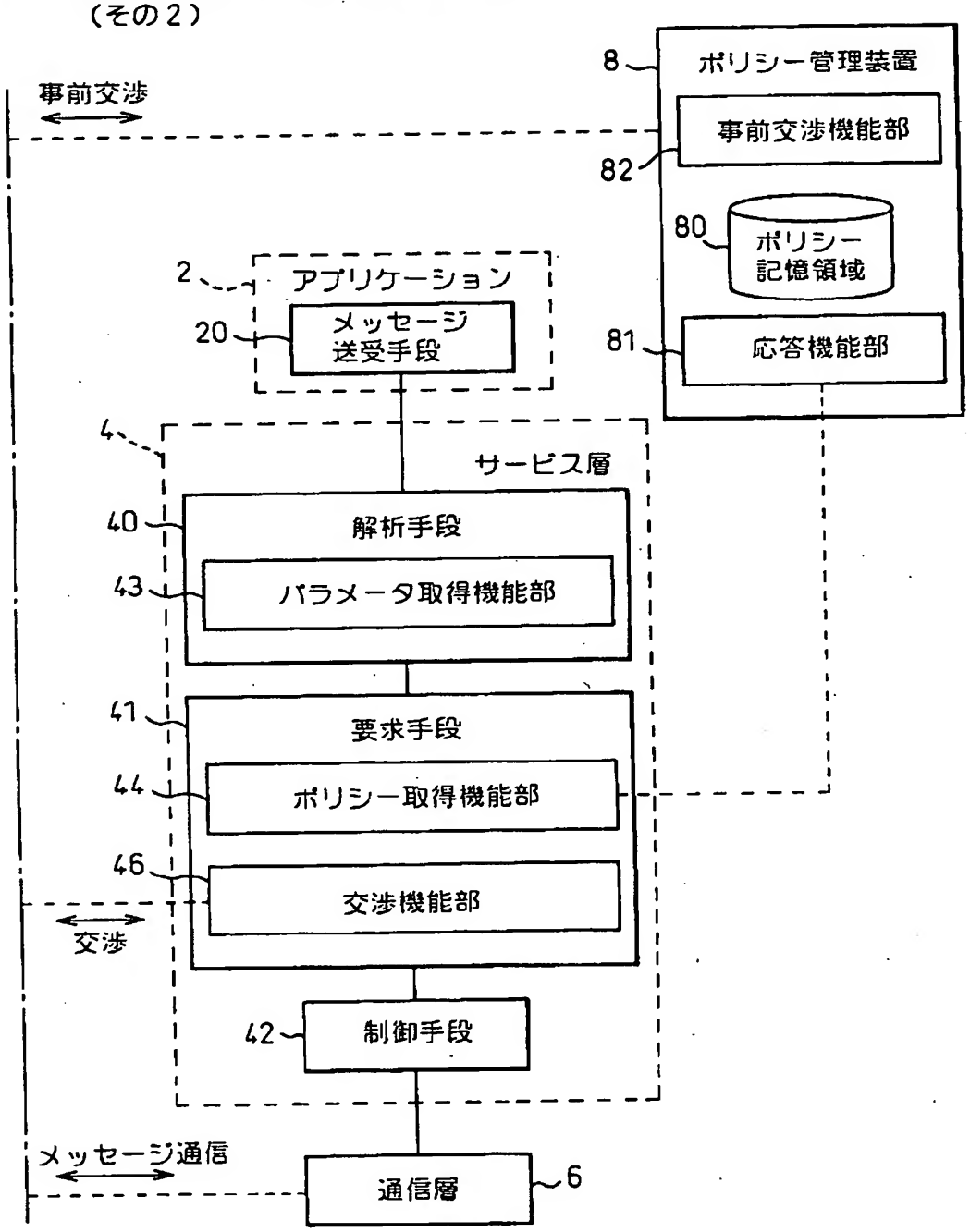
【図１２】

図12 既に提案されている、分散環境形のコンピュータシステムを示す図（その１）



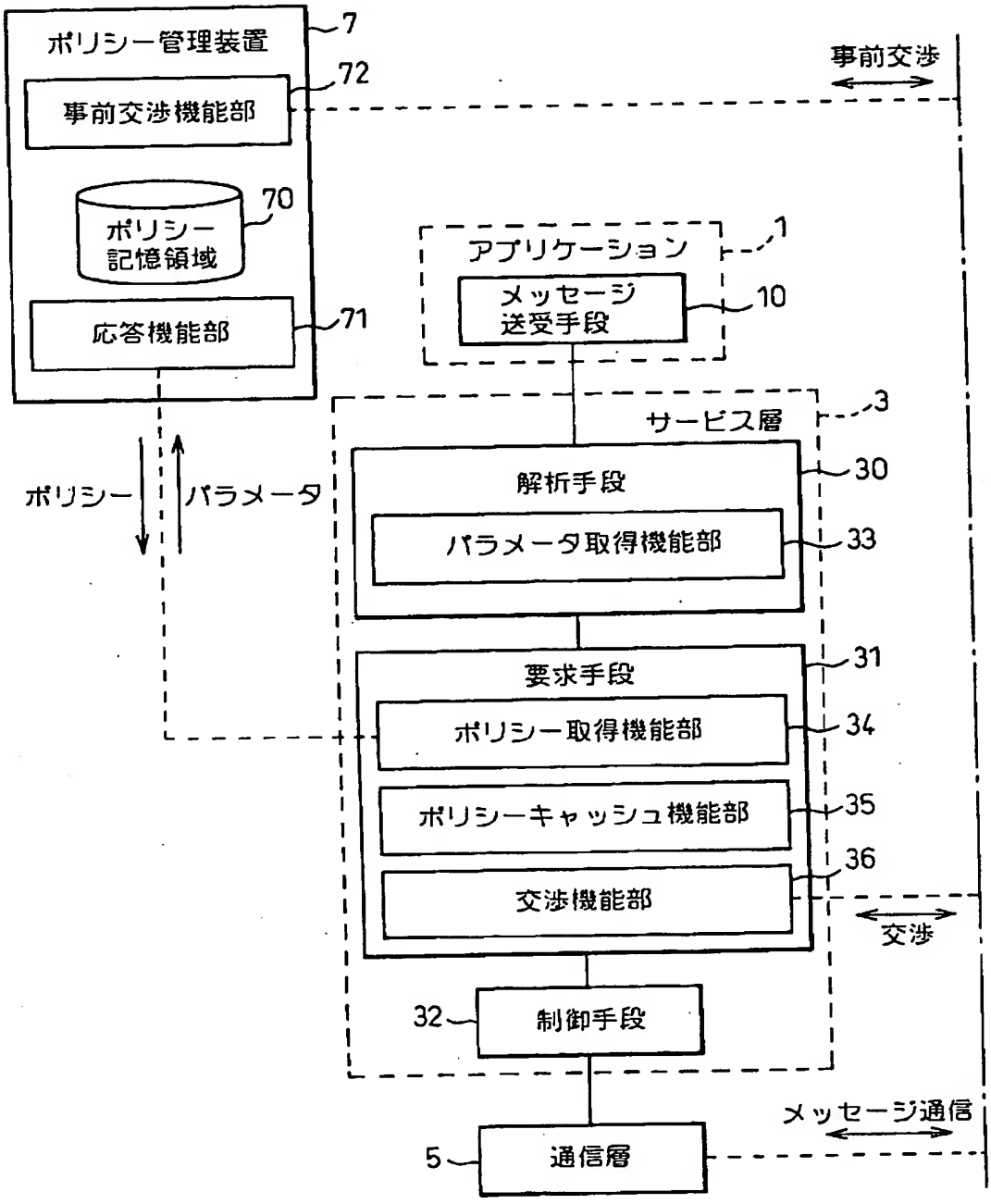
【図１３】

図13 既に提案されている、分散環境形のコンピュータシステムを示す図（その２）



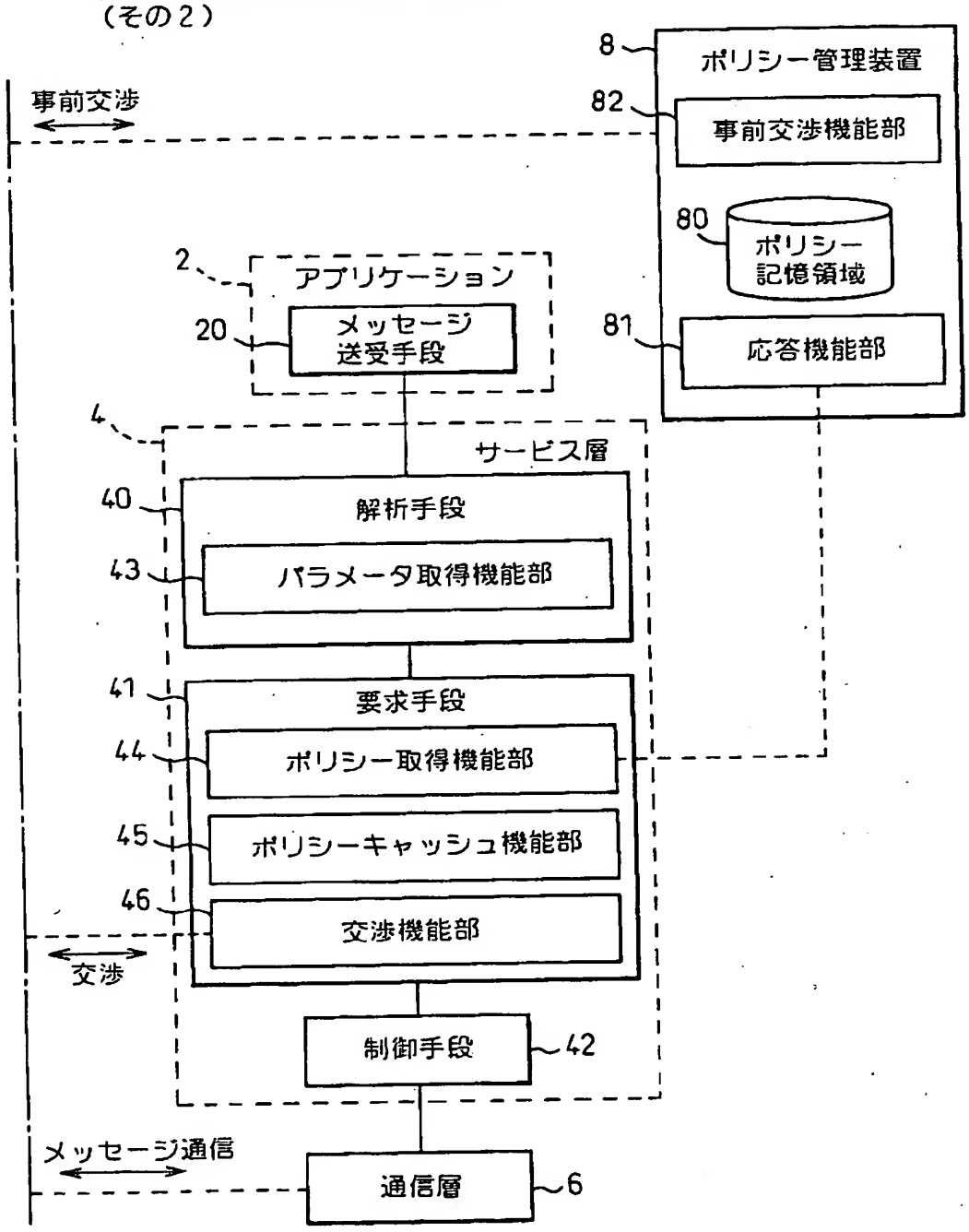
【図１４】

図14 本発明の前提をなす分散環境形のコンピュータシステムを示す図（その１）



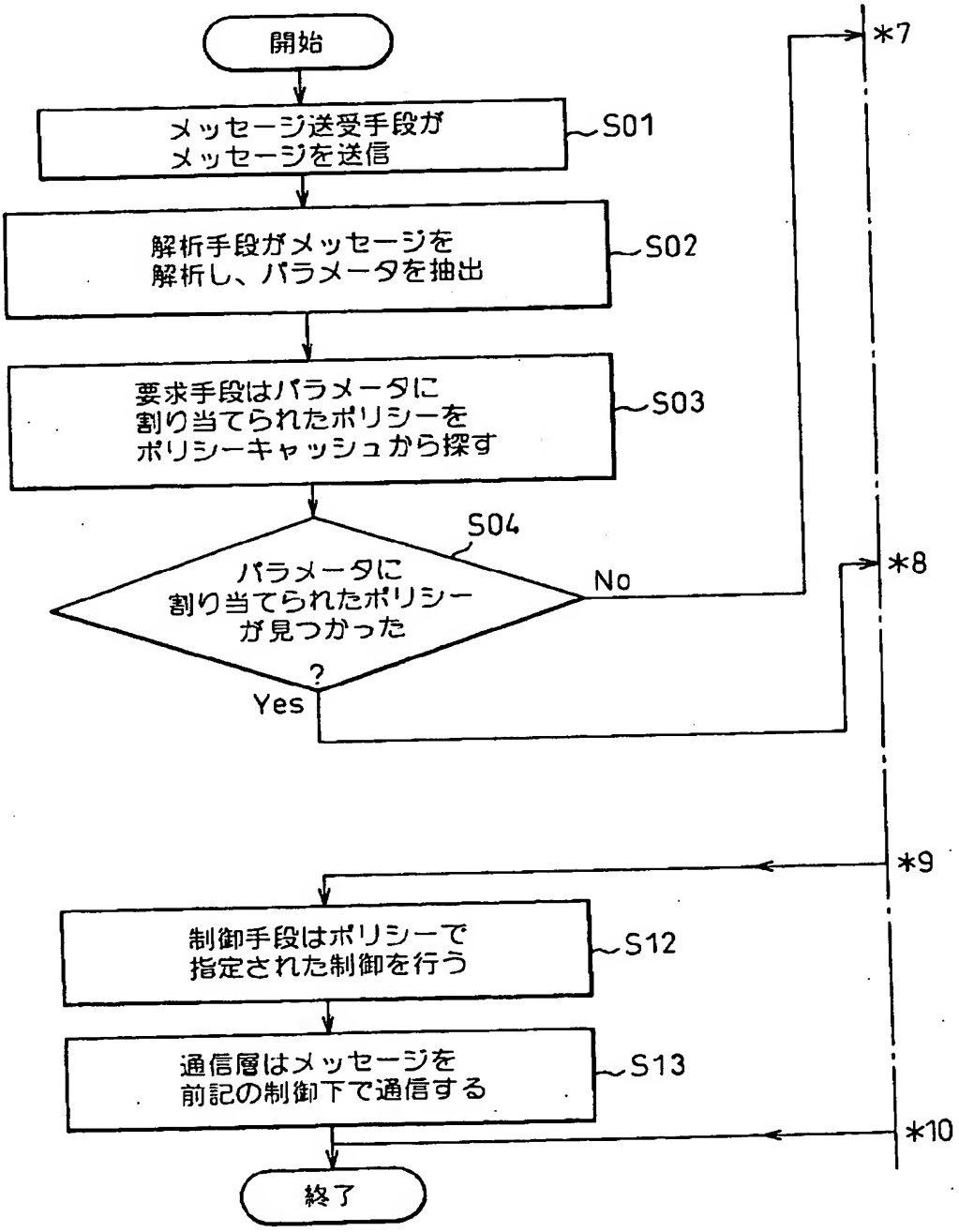
【図１５】

図15　本発明の前提をなす分散環境形のコンピュータシステムを示す図（その２）



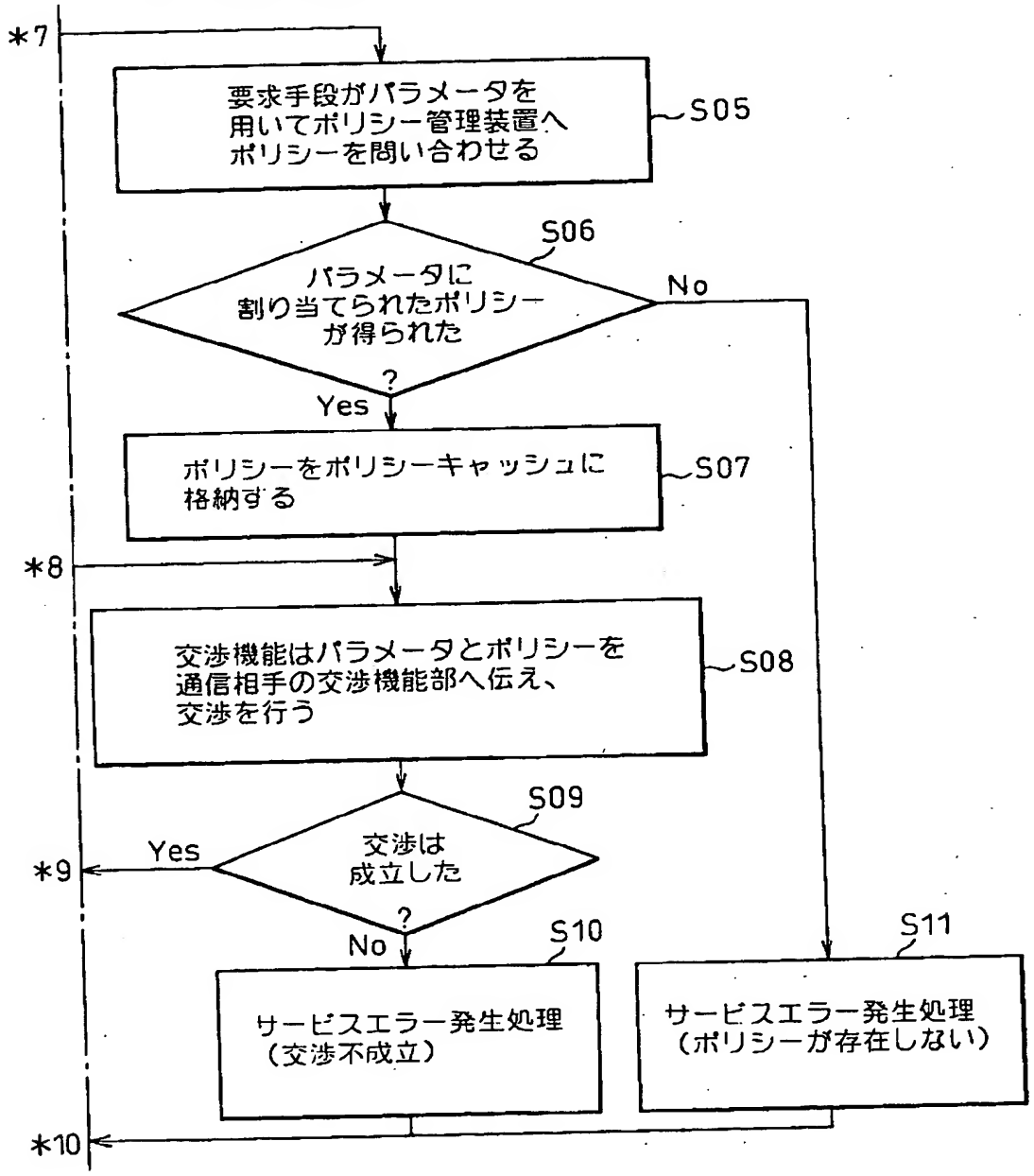
【図１６】

図16 図14および図15に示す本発明の前提をなすコンピュータシステムにおける処理の流れを示すフローチャート（その１）



【図１７】

図17　図14および図15に示す本発明の前提をなすコンピュータシステムにおける処理の流れを示すフローチャート（その２）



【書類名】　　要約書

【要約】

【課題】　サービス層が連続したメッセージ通信を高速に実行することのできる分散環境形のコンピュータシステムを提供する。

【解決手段】　メッセージ送受信手段１０と、ポリシーに従って、アプリケーション１に対し特定の付加的サービスを提供するサービス層３と、ポリシーを供給するポリシー管理装置７と、メッセージをやりとりする通信層と、を備えるコンピュータシステムであって、ここにメッセージに記述されるパラメータを、静的パラメータ１０１と動的パラメータ１０２とに区分して、メッセージより抽出する解析手段３０と、その静的パラメータを用いて、ポリシー管理装置７に対し、静的パラメータに割り当てられたポリシー群の取得を要求する要求手段３１と、を備えて構成する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社